

**INFORMATION RECORDING DEVICE AND INFORMATION  
REPRODUCING DEVICE AND ACCOUNTING DEVICE AND JUDGING  
DEVICE AND UPDATING DEVICE AND INFORMATION UTILIZING  
DEVICE AND KEY DISTRIBUTING DEVICE AND RECORDING MEDIUM**

**Patent number:** JP11283327 (A)

**Publication date:** 1999-10-15

**Inventor(s):** KAMIBAYASHI TATSU; AKIYAMA KOICHIRO; TSUJIMOTO  
SHUICHI; SUMITA KAZUO; HIRAKAWA HIDEKI; SUGAYA  
JUKO; KAJIURA MASAHIRO +

**Applicant(s):** TOSHIBA CORP +

**Classification:**

- international: **G06F12/14; G06F13/00; G06F21/00; G06F21/22; G06F21/24;  
G06F9/06; G09C1/00; G11B20/10;** (IPC1-7): G06F12/14;  
G06F13/00; G06F9/06; G09C1/00; G11B20/10

- european:

**Application number:** JP19980161660 19980513

**Priority number(s):** JP19980161660 19980513; JP19970122511 19970513;  
JP19980016618 19980129

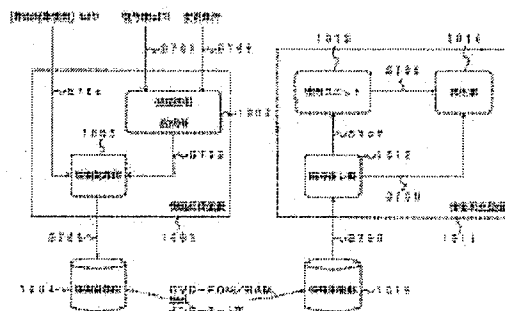
**Also published as:**

JP3792896 (B2)

**Abstract of JP 11283327 (A)**

**PROBLEM TO BE SOLVED:** To provide an information recording and reproducing device capable of constructing the utilization environment of digital information which assumes the protection of copyrights by accountings with respect to the utilization of the digital information easily.

**SOLUTION:** An information recording device 1001 generates license information by ciphering contents information and by ciphering a utilizing condition to be referred in order to limit the utilization of the contents information and a decoding key decoding the ciphered contents information to record the ciphered contents information and the generated license information on a recording medium.; An information reproducing device 1011 decodes the license information recorded on the recording medium by using a second decoding key for decoding the license information and judges whether the utilization of the contents information is possible or not based on the utilizing condition to be included in the decoded license information and when the utilization of the information is judged to be possible, the device 1011 decodes the ciphered contents information recorded on the recording medium by using a first decoding key to be included in the decoded license information.



Data supplied from the **espacenet** database — Worldwide



US 20020002466A1

(19) **United States**(12) **Patent Application Publication**  
**KAMBAYASHI et al.**(10) **Pub. No.: US 2002/0002466 A1**(43) **Pub. Date: Jan. 3, 2002**(54) **INFORMATION RECORDING APPARATUS,  
INFORMATION REPRODUCING  
APPARATUS, AND INFORMATION  
DISTRIBUTION SYSTEM**(30) **Foreign Application Priority Data**

May 13, 1997 (JP) ..... 9-122511

Jan. 29, 1998 (JP) ..... 10-016618

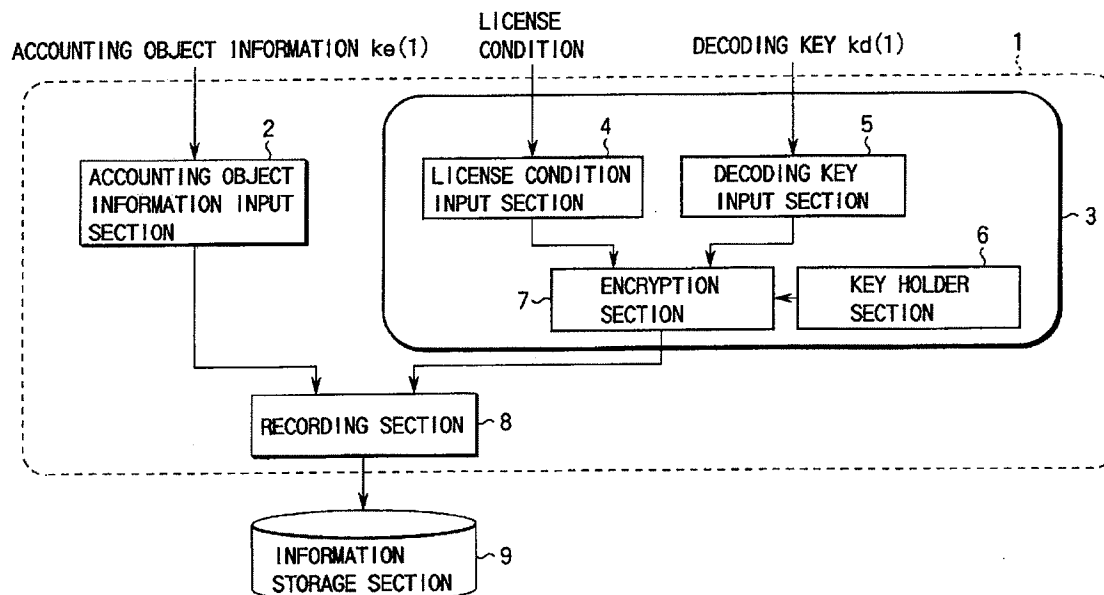
(76) **Inventors: TORU KAMBAYASHI,  
CHIGASAKI-SHI (JP); KOICHIRO  
AKIYAMA, KANAGAWA-KEN (JP);  
SHUICHI TSUJIMOTO,  
YOKOHAMA-SHI (JP); KAZUO  
SUMITA, YOKOHAMA-SHI (JP);  
HIDEKI HIRAKAWA,  
YOKOHAMA-SHI (JP); TOSHIHIRO  
SUGAYA, IBARAKI-KEN (JP)****Publication Classification**(51) **Int. Cl.<sup>7</sup> ..... G06F 17/60**(52) **U.S. Cl. .... 705/1**(57) **ABSTRACT**

An information recording apparatus comprises an encryption section encrypting contents information and also a license condition referred to to limit use of the contents information and a decoding key for decoding the encrypted contents information to generate license information, and a recording section recording the encrypted contents information and the generated license information on a recording medium. An information reproducing apparatus comprises a decoder unit decoding the license information recorded on the recording medium using a second decoding key for decoding the license information and deciding on the basis of the license condition contained in the decoded license information whether the contents information can be used. If it is decided that the contents information can be used, the encrypted contents information recorded on the recording medium is decoded using the first decoding key contained in the decoded license information.

**Correspondence Address:**

**OBLON SPIVAK MCCLELLAND MAIER &  
NEUSTADT PC  
FOURTH FLOOR  
1755 JEFFERSON DAVIS HIGHWAY  
ARLINGTON, VA 22202 (US)**

(\*) **Notice:** This is a publication of a continued prosecution application (CPA) filed under 37 CFR 1.53(d).

(21) **Appl. No.: 09/076,826**(22) **Filed: May 13, 1998**

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-283327

(43) 公開日 平成11年(1999)10月15日

(51) Int.Cl. <sup>8</sup>	識別記号	F I	
G 1 1 B 20/10		G 1 1 B 20/10	H
G 0 6 F 9/06	5 5 0	G 0 6 F 9/06	5 5 0 A
			5 5 0 Z
12/14	3 2 0	12/14	3 2 0 F
			3 2 0 B

審査請求 未請求 請求項の数71 F D (全 232 頁) 最終頁に続く

(21) 出願番号	特願平10-161660	(71) 出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22) 出願日	平成10年(1998) 5月13日	(72) 発明者	上林 達 神奈川県川崎市幸区小向東芝町1番地 株 式会社東芝研究開発センター内
(31) 優先権主張番号	特願平9-122511	(72) 発明者	秋山 浩一郎 神奈川県川崎市幸区小向東芝町1番地 株 式会社東芝研究開発センター内
(32) 優先日	平9(1997) 5月13日	(72) 発明者	辻本 修一 神奈川県川崎市幸区小向東芝町1番地 株 式会社東芝研究開発センター内
(33) 優先権主張国	日本 (J P)	(74) 代理人	弁理士 鈴江 武彦 (外6名)
(31) 優先権主張番号	特願平10-16618		
(32) 優先日	平10(1998) 1月29日		
(33) 優先権主張国	日本 (J P)		

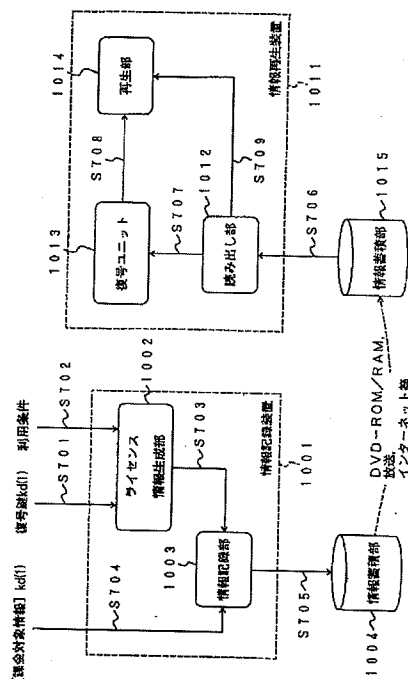
最終頁に続く

(54) 【発明の名称】 情報記録装置および情報再生装置および課金装置および判定装置および更新装置および情報利用装置および鍵配信装置および記録媒体

## (57) 【要約】

【課題】 デジタル情報の利用に対する課金による著作権の保護を前提としたデジタル情報の利用環境を容易に構築できる情報記録・再生装置を提供する。

【解決手段】 情報記録装置は、コンテンツ情報を暗号化して、該コンテンツ情報の利用を制限するために参照される利用条件と暗号化されたコンテンツ情報を復号する復号鍵とを暗号化してライセンス情報を生成し、暗号化されたコンテンツ情報と生成されたライセンス情報を記録媒体に記録する。情報再生装置は、ライセンス情報を復号するための第2の復号鍵を用いて前記記録媒体に記録されているライセンス情報を復号し、復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定して、前記コンテンツ情報の利用が可能と判定されたとき、復号されたライセンス情報に含まれる第1の復号鍵を用いて前記記録媒体に記録されている暗号化されたコンテンツ情報を復号する。



## 【特許請求の範囲】

【請求項1】 コンテンツ情報を暗号化する暗号化手段と、

少なくとも前記コンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号する復号鍵とを含む暗号化されたライセンス情報を生成するライセンス情報生成手段と、

前記暗号化手段で暗号化されたコンテンツ情報と前記ライセンス情報生成手段で生成されたライセンス情報とを記録媒体に記録する記録手段と、

を具備したことを特徴とする情報記録装置。

【請求項2】 コンテンツ情報から一部の情報を分離する分離手段と、

少なくとも、前記分離手段で分離された前記一部の情報と前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化されたライセンス情報を生成するライセンス情報生成手段と、

このライセンス情報生成手段で生成されたライセンス情報と前記コンテンツ情報の他の一部を記録媒体に記録する記録手段と、

を具備したことを特徴とする情報記録装置。

【請求項3】 コンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化された記録情報を生成する記録情報生成手段と、この記録情報生成手段で生成された記録情報を記録媒体に記録する記録手段と、

を具備したことを特徴とする情報記録装置。

【請求項4】 暗号化されたコンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件および前記コンテンツ情報を復号するための第1の鍵情報を含む暗号化されたライセンス情報とが記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、

前記ライセンス情報を復号するための第2の鍵情報を記憶する記憶手段と、

この記憶手段に記憶されている第2の鍵情報を用いて前記記録媒体に記録されているライセンス情報を復号する第1の復号手段と、

この第1の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記第1の復号手段で復号されたライセンス情報に含まれる第1の鍵情報を用いて前記記録媒体に記録されているコンテンツ情報を復号する第2の復号手段と、

を具備したことを特徴とする情報再生装置。

【請求項5】 コンテンツ情報の一部と、少なくとも前記コンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報の他の一部を含む暗号化されたライセ

ンス情報とが記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、

前記ライセンス情報を復号する鍵情報を記憶する記憶手段と、

この記憶手段に記憶されている鍵情報を用いて前記記録媒体に記録されているライセンス情報を復号する復号手段と、

この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる前記コンテンツ情報の一部と、前記記録媒体に記録されている前記コンテンツ情報の一部とを合成して前記コンテンツ情報を再生する再生手段と、を具備したことを特徴とする情報再生装置。

【請求項6】 少なくともコンテンツ情報と前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化された記録情報が記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、前記記録情報を復号するための鍵情報を記憶する記憶手段と、

この記憶手段に記憶されている鍵情報を用いて前記記録媒体に記録されている記録情報を復号する復号手段と、

この復号手段で復号された記録情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたコンテンツ情報を再生する再生手段と、

を具備したことを特徴とする情報再生装置。

【請求項7】 前記利用条件は少なくとも前記コンテンツ情報の利用期限を含み、

前記判定手段は、日時を計測する計測手段を具備し、この計測手段で計測された日時と前記利用期限とを比較して前記コンテンツ情報の利用の可否を判定することを特徴とする請求項4～6のいずれか1つに記載の情報再生装置。

【請求項8】 前記利用条件は少なくとも前記コンテンツ情報の利用期限を含み、

前記判定手段は、

日時を計測する計測手段と、

この計測手段で計測される日時の更新を無効化する更新無効化手段と、

を具備し、前記計測手段で計測された日時と前記利用期限とを比較して前記コンテンツ情報の利用の可否を判定することを特徴とする請求項4～6のいずれか1つに記載の情報再生装置。

【請求項9】 前記利用条件は少なくとも前記コンテンツ情報の利用期限を含み、



前記判定手段は、  
日時を計測する計測手段と、  
前記計測手段で計測される日時を更新するための暗号化された更新情報を受信する受信手段と、  
この受信手段で受信された暗号化された更新情報を復号し、その復号された更新情報に基づき、前記計測手段で計測される日時を更新する更新手段と、  
を具備し、前記計測手段で計測された日時と前記利用期限とを比較して前記コンテンツ情報の利用の可否を判定することを特徴とする請求項4～6のいずれか1つに記載の情報再生装置。

【請求項10】 前記利用条件は少なくとも前記コンテンツ情報の利用期限と前記記録媒体への情報の記録日時を含み、  
前記判定手段は、日時を計測する計測手段を具備し、この計測手段で計測された日時と前記利用期限と前記記録日時とを比較して前記コンテンツ情報の利用の可否を判定することを特徴とする請求項4～6のいずれか1つに記載の情報再生装置。

【請求項11】 前記利用条件は少なくとも前記コンテンツ情報を識別するためのコンテンツ情報識別子を含み、  
前記判定手段で前記コンテンツ情報の利用が不可と判定されたとき、前記コンテンツ情報識別子に対応するコンテンツ情報の利用に対する料金の支払いを要求する要求手段と、  
前記要求に応じて料金の支払いが確認されたとき、前記記録媒体に記録されている少なくとも利用条件を更新する更新手段と、  
を具備したことを特徴とする請求項4～6のいずれか1つに記載の情報再生装置。

【請求項12】 前記利用条件は少なくとも前記コンテンツ情報の利用期限を含み、  
前記利用条件に前記ライセンス情報を復号できるユニットを限定するための前記ユニットを識別するための復号ユニット識別子が含まれていないとき、前記ライセンス情報を復号できるユニットの復号ユニット識別子を前記利用条件に追加する利用条件更新手段を具備し、  
前記判定手段は、前記利用期限と前記復号ユニット識別子に基づき前記コンテンツ情報の利用の可否を判定することを特徴とする請求項4～5のいずれか1つに記載の情報再生装置。

【請求項13】 前記利用条件は少なくとも前記コンテンツ情報の利用期限を含み、  
前記利用条件に前記記録情報を復号できるユニットを限定するための前記ユニットを識別するための復号ユニット識別子が含まれていないとき、前記記録情報を復号できるユニットの復号ユニット識別子を前記利用条件に追加する利用条件更新手段を具備し、  
前記判定手段は、前記利用期限と前記復号ユニット識別

子に基づき前記コンテンツ情報の利用の可否を判定することを特徴とする請求項6記載の情報再生装置。

【請求項14】 前記利用条件は少なくとも前記コンテンツ情報を記録できる記録媒体を識別するための媒体識別子を含み、

前記判定手段は、さらに、前記媒体識別子に基づき前記コンテンツ情報の利用の可否を判定することを特徴とする請求項4～6のいずれか1つに記載の情報再生装置。

【請求項15】 記録媒体に記録されたコンテンツ情報の利用に対する課金を行う課金装置において、  
記録媒体に記録されたコンテンツ情報の利用条件を入力する入力手段と、

この入力手段で入力された利用条件に基づき前記コンテンツ情報の利用に対する料金の支払いを要求する要求手段と、

前記要求に応じて料金の支払いが確認されたとき、少なくとも前記入力手段で入力された利用条件を含むライセンス情報を前記記録媒体に記録する記録手段と、  
を具備したことを特徴とする課金装置。

【請求項16】 コンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件を含む暗号化されたライセンス情報とが記録された記録媒体を介した前記コンテンツ情報の利用に対する課金を行う課金装置において、

前記記録媒体に記録された暗号化されたライセンス情報を入力する入力手段と、

この入力手段で入力された暗号化されたライセンス情報を復号する復号手段と、

前記コンテンツ情報を利用するための利用条件を入力する利用条件入力手段と、この利用条件入力手段で入力された利用条件に基づき前記コンテンツ情報の利用に対する料金の支払いを要求する要求手段と、

前記要求に応じて料金の支払いが確認されたとき、前記利用条件入力手段で入力された利用条件に基づき前記復号手段で復号されたライセンス情報を更新する更新手段と、

この更新手段で更新されたライセンス情報を暗号化する暗号手段と、

この暗号手段で暗号化されたライセンス情報を出力する出力手段と、

を具備したことを特徴とする課金装置。

【請求項17】 少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、

前記ライセンス情報を復号する第2の鍵情報を予め定められた時間毎に生成する鍵生成手段と、

入力された前記ライセンス情報を前記鍵生成手段で生成された第2の鍵情報を用いて復号する復号手段と、

この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第1の鍵情報を出力する出力手段と、を具備したことを特徴とする判定装置。

【請求項18】 前記鍵生成手段は、前記ライセンス情報を暗号化する際に用いる公開鍵とそれに対応する該ライセンス情報を復号するための秘密鍵とを生成し、前記判定手段で前記コンテンツ情報の利用が不可と判定されたとき、少なくとも新たに指定された利用条件と前記鍵生成手段で新たに生成された公開鍵とを通知して前記ライセンス情報の更新を要求する更新要求手段と、を具備し、前記更新要求手段でのライセンス情報の更新要求を受けて更新されたライセンス情報は該更新要求の際に通知された前記鍵生成手段で新たに生成された公開鍵で暗号化されることを特徴とする請求項17記載の判定装置。

【請求項19】 少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第1の鍵情報と該暗号化された第1の鍵情報を復号するための第2の鍵情報を生成するために必要な第1の鍵生成情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、前記ライセンス情報を復号する復号手段と、この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる暗号化された第1の鍵情報と第1の鍵生成情報とを出力する出力手段と、を具備したことを特徴とする判定装置。

【請求項20】 前記判定手段で前記コンテンツ情報の利用が不可と判定されたとき、少なくとも新たに指定された利用条件と該コンテンツ情報の利用装置から取得した該利用装置に固有の前記第2の鍵情報を生成するために必要な第2の鍵生成情報とを通知して前記ライセンス情報の更新を要求する更新要求手段と、を具備し、前記更新要求手段でのライセンス情報の更新要求を受けて、前記利用条件と前記第1の鍵生成情報と前記第2の鍵情報とが更新されることを特徴とする請求項19記載の判定装置。

【請求項21】 少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための暗号化された第1の鍵情報と該暗号化された第1の鍵情報を復号するための第2の鍵情報を生成するために

必要な第1の鍵生成情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、

前記ライセンス情報を復号する第3の鍵情報を予め定められた時間毎に生成する鍵生成手段と、

入力された前記ライセンス情報を前記鍵生成手段で生成された第3の鍵情報を用いて復号する復号手段と、

この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる暗号化された第1の鍵情報と第1の鍵生成情報とを出力する出力手段と、を具備したことを特徴とする判定装置。

【請求項22】 前記鍵生成手段は、前記ライセンス情報を暗号化する際に用いる公開鍵とそれに対応する該ライセンス情報を復号するための秘密鍵とを生成し、前記判定手段で前記コンテンツ情報の利用が不可と判定されたとき、少なくとも、新たに指定された利用条件と該コンテンツ情報の利用装置から取得した該利用装置に固有の前記第2の鍵情報を生成するために必要な第2の鍵生成情報と前記鍵生成手段で新たに生成された公開鍵とを通知して前記ライセンス情報の更新を要求する更新要求手段と、

を具備し、前記更新要求手段でのライセンス情報の更新要求を受けて、前記利用条件と前記第1の鍵生成情報と前記第2の鍵情報とが更新され、該更新されたライセンス情報は、該更新要求の際に通知された前記鍵生成手段で新たに生成された公開鍵で暗号化されることを特徴とする請求項21記載の判定装置。

【請求項23】 少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを第2の鍵情報で暗号化したものと、少なくとも該第2の鍵情報を生成するために必要な鍵生成情報とを含むライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置において、入力された前記ライセンス情報に含まれる鍵生成情報に基づき前記第2の鍵情報を生成する鍵生成手段と、この鍵生成手段で生成された第2の鍵情報を用いて前記ライセンス情報に含まれる利用条件と第1の鍵情報とを復号する復号手段と、この復号手段で復号された利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号された第1の鍵情報を出力する出力手段と、を具備したことを特徴とする判定装置。

【請求項24】 少なくともコンテンツ情報の利用を制

限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを第2の鍵情報で暗号化したものと、少なくとも該第2の鍵情報を生成するために必要な2つの鍵生成情報とを含むライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置において、  
入力された前記ライセンス情報に含まれる前記2つの鍵生成情報に基づき前記第2の鍵情報を生成する鍵生成手段と、  
この鍵生成手段で生成された第2の鍵情報を用いて前記ライセンス情報に含まれる利用条件と第1の鍵情報とを復号する復号手段と、  
この復号手段で復号された利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、  
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号された第1の鍵情報を出力する出力手段と、  
前記判定手段で前記コンテンツ情報の利用が不可と判定されたとき、少なくとも前記2つの鍵生成情報のうちの一方あるいは該一方の鍵生成情報を更新したものと新たに指定された利用条件とを通知して前記ライセンス情報の更新を要求する更新要求手段と、  
を具備し、前記更新要求手段でのライセンス情報の更新要求を受けて、前記利用条件と他方の鍵生成情報と前記第2の鍵情報とが更新されることを特徴とする判定装置。

【請求項25】 少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための鍵情報とを含む公開鍵で暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と更新された公開鍵とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、  
前記更新されたライセンス情報を前記通知された公開鍵で暗号化することを特徴とする更新装置。

【請求項26】 少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第1の鍵情報と該暗号化された第1の鍵情報を復号する第2の鍵情報を生成するために必要な第1の鍵生成情報とを含む暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と前記第2の鍵情報を生成するために必要な第2の鍵生成情報とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、  
前記利用条件と前記第1の鍵生成情報とを更新し、該更新された第1の鍵生成情報と前記第2の鍵生成情報とに基づき前記第2の鍵情報を更新し、この更新された第2

の鍵情報で前記第1の鍵情報を暗号化して、少なくとも該更新された利用条件と該更新された第2の鍵情報で暗号化された第1の鍵情報と該更新された第1の鍵生成情報とを含む暗号化されたライセンス情報を生成することを特徴とする更新装置。

【請求項27】 少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第1の鍵情報と該暗号化された第1の鍵情報を復号する第2の鍵情報を生成するために必要な第1の鍵生成情報とを含む公開鍵で暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と前記第2の鍵情報を生成するために必要な第2の鍵生成情報と更新された公開鍵とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、  
前記利用条件と前記第1の鍵生成情報とを更新し、該更新された第1の鍵生成情報と前記第2の鍵生成情報とに基づき前記第2の鍵情報を更新し、この更新された第2の鍵情報で前記第1の鍵情報を暗号化して、少なくとも該更新された利用条件と該更新された第2の鍵情報で暗号化された第1の鍵情報と該更新された第1の鍵生成情報とを含むライセンス情報を生成し、この生成されたライセンス情報を前記通知された公開鍵で暗号化することを特徴とする更新装置。

【請求項28】 少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための第1の鍵情報とを第2の鍵情報で暗号化したものと、少なくとも該第2の鍵情報を生成するために必要な2つの鍵生成情報とを含むライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも前記2つの鍵生成情報のうちの一方あるいは該一方の鍵生成情報を更新したものと新たに指定された利用条件とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、  
前記利用条件と他方の鍵生成情報とを更新し、該更新された他方の鍵生成情報と前記通知された一方の鍵生成情報とに基づき前記第2の鍵情報を更新して、少なくとも該更新された利用条件と該第1の鍵情報とを該更新された第2の鍵情報で暗号化したものと、少なくとも前記通知された一方の鍵生成情報と該更新された他方の鍵生成情報とを含むライセンス情報を生成することを特徴とする更新装置。

【請求項29】 暗号化されたコンテンツ情報を復号するための暗号化された第1の鍵情報と該第1の鍵情報を復号する第2の鍵情報を生成するために必要な第1の鍵生成情報とが入力されて、該コンテンツ情報を復号および利用する情報利用装置において、  
前記第1の鍵情報を復号する第2の鍵情報を生成するた

めに必要な第2の鍵生成情報を保持し、この第2の鍵生成情報と前記入力された第1の鍵生成情報とに基づき前記第2の鍵情報を生成し、この生成された第2の鍵情報を用いて前記暗号化されたコンテンツ情報を復号することを特徴とする情報利用装置。

【請求項30】 記録媒体に記録された暗号化されたコンテンツ情報を該記録媒体に記憶された、少なくとも前記コンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき復号および利用する情報利用装置において、

日時を計測する計測手段と、

この計測手段で計測された日時と前記記録媒体に記録されたライセンス情報とに基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

前記判定手段で前記コンテンツ情報の利用が可能と判定されたとき該判定手段から出力される前記第1の鍵情報を用いて前記記録媒体に記録されたコンテンツ情報を復号する復号手段と、

を具備し、

前記計測手段から前記判定手段へ日時を通知するための情報と、前記判定手段から前記復号手段へ出力される第1の鍵情報とは暗号化されていることを特徴とする情報利用装置。

【請求項31】 前記判定手段は着脱可能であることを特徴とする請求項30記載の情報利用装置。

【請求項32】 前記計測手段から前記判定手段へ日時を通知するための情報は、暗号および復号で共通の鍵情報を用いて暗号化されることを特徴とする請求項30記載の情報利用装置。

【請求項33】 前記計測手段から前記判定手段へ日時を通知するための情報は、前記計測手段と前記判定手段のそれぞれで生成される鍵情報を用いて暗号化および復号化されることを特徴とする請求項30記載の情報利用装置。

【請求項34】 前記計測手段から前記判定手段へ日時を通知するための情報は、前記計測手段と前記判定手段とがそれぞれ保持する第1の鍵生成情報と互いに通知しあった乱数とに基づき生成される鍵情報を用いて暗号化および復号化されることを特徴とする請求項30記載の情報利用装置。

【請求項35】 前記判定手段から前記復号手段へ出力される第1の鍵情報は、暗号および復号で共通の鍵情報を用いて暗号化されることを特徴とする請求項30記載の情報利用装置。

【請求項36】 前記判定手段から前記復号手段へ出力される第1の鍵情報は、前記判定手段と前記復号手段のそれぞれで生成される鍵情報を用いて暗号化および復号化されることを特徴とする請求項30記載の情報利用装置。

【請求項37】 前記判定手段から前記復号手段へ出力される第1の鍵情報は、前記判定手段と前記復号手段のそれぞれで保持する第2の鍵生成情報と互いに通知しあった乱数とに基づき生成される鍵情報を用いて暗号化および復号化されることを特徴とする請求項30記載の情報利用装置。

【請求項38】 前記判定手段は、前記日時を通知するための情報を復号した際、そのデータ形式が予め定められた形式であるときのみ該情報を前記コンテンツ情報の利用の可否の判定に用いることを特徴とする請求項30記載の情報利用装置。

【請求項39】 前記判定手段は、前記日時を通知するための情報が到着するまでの時間を計測して、該時間が予め定められた時間内であるときのみ該情報を前記コンテンツ情報の利用の可否の判定に用いることを特徴とする請求項30記載の情報利用装置。

【請求項40】 前記判定手段は、前記ライセンス情報を暗号化する第2の鍵情報とそれに対応する前記ライセンス情報を復号する第3の鍵情報との対を記憶する記憶手段と、

前記記録媒体に記録された前記第3の鍵情報の識別情報を基に前記記憶手段から第3の鍵情報を検索して前記ライセンス情報を復号する第2の復号手段と、

を具備し、

前記記憶手段に記憶されている第2の鍵情報と第3の鍵情報との対の少なくとも一部は更新されることを特徴とする請求項30記載の情報再生装置。

【請求項41】 前記判定手段は、前記ライセンス情報を暗号化する第2の鍵情報とそれに対応する前記ライセンス情報を復号する第3の鍵情報との対を記憶する記憶手段と、

前記記録媒体に記録された前記第3の復号鍵の識別情報を基に前記記憶手段から第3の鍵情報を検索して前記ライセンス情報を復号する第2の復号手段と、を具備し、前記記憶手段に記憶されている第2の鍵情報と第3の鍵情報との対の少なくとも一部は各判定手段で固有であることを特徴とする請求項30記載の情報利用装置。

【請求項42】 暗号化されたコンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件および前記コンテンツ情報を復号するための第1の鍵情報を含む暗号化されたライセンス情報とが記録された記録媒体から読み出された該暗号化されたライセンス情報と、日時を通知するための暗号化された日時情報とを入力して、前記コンテンツ情報の利用の可否を判定する判定装置であって、

前記暗号化されたライセンス情報を復号する第1の復号手段と、

前記暗号化された日時情報を復号する第2の復号手段と、

前記第1および第2の復号手段で復号された情報に基づ

き前記コンテンツ情報の利用の可否を判定する判定手段と、  
この判定手段で前記コンテンツ情報の利用が可能と判定されたとき前記第1の鍵情報を暗号化して出力する出力手段と、  
を具備し、演算機能を有する携帯可能記録媒体で構成されたことを特徴とする判定装置。

【請求項43】 前記第2の復号手段は、予め保持されている第1の鍵生成情報と乱数とに基づき生成される鍵情報を用いて復号することを特徴とする請求項42記載の判定装置。

【請求項44】 前記判定手段は、前記第2の復号手段で復号された日時情報のデータ形式が予め定められた形式であるときのみ該日時情報を前記コンテンツ情報の利用の可否の判定に用いることを特徴とする請求項42記載の判定装置。

【請求項45】 前記判定手段は、前記暗号化された日時情報が到着するまでの時間を計測して、該時間が予め定められた時間内であるときのみ該日時情報を前記コンテンツ情報の利用の可否の判定に用いることを特徴とする請求項42記載の判定装置。

【請求項46】 前記付加情報を暗号化する第2の鍵情報とそれに対応する前記ライセンス情報を復号する第3の鍵情報との対を記憶する記憶手段を具備し、  
前記第1の復号手段は、前記記録媒体から読み出された前記第3の鍵情報を指定するための識別情報を基に前記記憶手段から第3の鍵情報を検索して前記ライセンス情報を復号し、前記記憶手段に記憶されている第2の鍵情報と第3の鍵情報との対の少なくとも一部は更新されることを特徴とする請求項42記載の判定装置。

【請求項47】 前記ライセンス情報を暗号化する第2の鍵情報とそれに対応する前記ライセンス情報を復号する第3の鍵情報との対を記憶する記憶手段を具備し、  
前記第1の復号手段は、前記記録媒体に記録された前記第3の鍵情報の識別情報を基に前記記憶手段から第3の鍵情報を検索して前記ライセンス情報を復号し、前記記憶手段に記憶されている第2の鍵情報と第3の鍵情報との対の少なくとも一部は更新されることを特徴とする請求項42記載の判定装置。

【請求項48】 前記ライセンス情報を暗号化する第2の鍵情報とそれに対応する前記ライセンス情報を復号する第3の鍵情報との対を記憶する記憶手段を具備し、  
前記第1の復号手段は、前記記録媒体に記録された前記第3の鍵情報の識別情報を基に前記記憶手段から第3の鍵情報を検索して前記ライセンス情報を復号し、前記記憶手段に記憶されている第2の鍵情報と第3の鍵情報との対の少なくとも一部は各判定装置で固有であることを特徴とする請求項42記載の判定装置。

【請求項49】 前記鍵生成手段は、予め定められた時間毎に当該時刻情報に基づき第2の鍵情報を生成するこ

とを特徴とする請求項17記載の判定装置。

【請求項50】 前記鍵生成手段は、予め定められた時間毎に当該時刻情報に基づき第3の鍵情報を生成することを特徴とする請求項21記載の判定装置。

【請求項51】 前記復号手段で復号された前記ライセンス情報には、復号結果の正否を判定するための認証情報が含まれていることを特徴とする請求項17または19または21または23または24記載の判定装置。

【請求項52】 少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、

前記ライセンス情報を復号する第2の鍵情報を放送配信される第1の鍵生成情報に基づき生成する鍵生成手段と、

入力された前記ライセンス情報を前記鍵生成手段で生成された第2の鍵情報を用いて復号する復号手段と、

この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第1の鍵情報を出力する出力手段と、  
を具備したことを特徴とする判定装置。

【請求項53】 入力された前記暗号化ライセンス情報を記憶する記憶手段と、

この記憶手段に記憶された暗号化ライセンス情報から前記コンテンツ情報に対応する前記暗号化ライセンス情報を選択する選択手段と、

前記復号手段は、この選択手段で選択された暗号化ライセンス情報を復号することを特徴とする請求項17または52記載の判定装置。

【請求項54】 入力された前記暗号化ライセンス情報を記憶する記憶手段と、

この記憶手段に記憶された暗号化ライセンス情報から該ライセンス情報の種別の予め定められた優先順位に基づき、前記コンテンツ情報に対応する暗号化ライセンス情報を選択する選択手段と、

前記復号手段は、この選択手段で選択された暗号化ライセンス情報を復号することを特徴とする請求項17または52記載の判定装置。

【請求項55】 記録媒体に記録された暗号化されたコンテンツ情報を復号するために必要な第1の鍵情報を前記コンテンツ情報を利用する情報利用装置へ配信する鍵配信装置において、

前記情報利用装置との間で共有される第1の秘密パラメータを記憶する第1の記憶手段と、

この第1の記憶手段に記憶された第1の秘密パラメータと、該情報利用装置との間で交換される第1の公開パラ

メータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、  
少なくとも前記第1の鍵情報を含む暗号化された第1の暗号情報を、前記第1の鍵生成手段で生成された第2の鍵情報で暗号化する暗号手段と、  
この暗号手段で暗号化された少なくとも前記第1の暗号情報を含む第2の暗号情報を前記情報利用装置に配信する配信手段と、  
を具備したことを特徴とする鍵配信装置。

【請求項56】 前記第1の暗号情報には、前記コンテンツ情報の利用を制限するための利用条件が含まれていることを特徴とする請求項55記載の鍵配信装置。

【請求項57】 前記第2の暗号情報には、前記コンテンツ情報の利用を制限するための利用条件が含まれていることを特徴とする請求項55記載の鍵配信装置。

【請求項58】 前記情報利用装置との間で共有される第2の秘密パラメータを記憶する第2の記憶手段と、  
前記情報利用装置から暗号化された該情報利用装置の識別情報を受信する受信手段と、  
前記第2の記憶手段に記憶された第2の秘密パラメータと前記情報利用装置との間で交換される第2の公開パラメータとに基づき第3の鍵情報を生成する第2の鍵生成手段と、  
前記受信手段で受信された暗号化された前記情報利用装置の識別情報を前記第2の鍵生成手段で生成された第3の鍵情報を用いて復号する第1の復号手段と、前記暗号手段は、この第1の復号手段で復号された前記情報利用装置の識別情報を前記第1の暗号情報とともに前記第2の鍵情報で暗号化して第2の暗号情報を生成することを特徴とする請求項55記載の鍵配信装置。

【請求項59】 前記情報利用装置との間の通信は、演算機能を有する記録媒体を介して行われることを特徴とする請求項55記載の鍵配信装置。

【請求項60】 前記情報利用装置との間の通信は、演算機能を有する記録媒体を介して行われ、  
前記記録媒体との間で共有される第3の秘密パラメータを記憶する第3の記憶手段と、  
前記記録媒体から暗号化された該記録媒体の識別情報を受信する受信手段と、前記第3の記憶手段に記憶された第3の秘密パラメータと、前記記録媒体との間で交換される第3の公開パラメータとに基づき第4の鍵情報を生成する第3の鍵生成手段と、  
前記受信手段で受信された暗号化された前記記録媒体の識別情報を前記第3の鍵生成手段で生成された第3の鍵情報を用いて復号する第2の復号手段と、  
前記暗号手段は、この第2の復号手段で復号された前記記録媒体の識別情報を前記第1の暗号情報とともに前記第2の鍵情報で暗号化して第2の暗号情報を生成することを特徴とする請求項55記載の鍵配信装置。

【請求項61】 少なくともコンテンツ情報の利用を制

限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、

前記ライセンス情報の配信装置との間で共有される第1の秘密パラメータを記憶する第1の記憶手段と、

この第1の記憶手段に記憶された第1の秘密パラメータと前記配信装置との間で交換される第1の公開パラメータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、

受信した前記暗号化されたライセンス情報を前記第1の鍵生成手段で生成された第2の鍵情報で復号する第1の復号手段と、

この第1の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、

この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第1の鍵情報を出力する出力手段と、  
を具備したことを特徴とする判定装置。

【請求項62】 前記出力手段は、  
前記コンテンツ情報を利用する情報利用装置との間で共有される第2の秘密パラメータを記憶する第2の記憶手段と、

この第2の記憶手段に記憶された第2の秘密パラメータと前記情報利用装置との間で交換される第2の公開パラメータとに基づき第3の鍵情報を生成する第2の鍵生成手段と、

この第2の鍵生成手段で生成された第3の鍵情報で前記第1の鍵情報を暗号化して前記情報利用装置へ出力することを特徴とする請求項61記載の判定装置。

【請求項63】 前記コンテンツ情報を利用する情報利用装置との間で共有される第3の秘密パラメータを記憶する第3の記憶手段と、

前記情報利用装置から前記コンテンツ情報の記録された第1の記録媒体の暗号化された識別情報を受信する第1の受信手段と、

前記第3の記憶手段に記憶された第3の秘密パラメータと前記情報利用装置との間で交換される第3の公開パラメータとに基づき第4の鍵情報を生成する第3の鍵生成手段と、

この第3の鍵生成手段で生成された第4の鍵情報で前記第1受信手段で受信された暗号化された識別情報を復号する第2の復号手段と、

前記判定手段は、この第2の復号手段で復号された識別情報と前記復号されたライセンス情報とに基づき前記コンテンツ情報の利用の可否を判定することを特徴とする請求項61記載の判定装置。

【請求項64】 前記配信装置との間の通信は、演算機能を有する記録媒体を介して行われることを特徴とする

請求項61記載の判定装置。

【請求項65】 前記配信装置との間の通信は、演算機能を有する記録媒体を介して行われ、前記該記録媒体との間で共有される第4の秘密パラメータを記憶する第4の記憶手段と、前記記録媒体から該記録媒体の暗号化された識別情報を受信する第2の受信手段と、前記第4の記憶手段に記憶された第4の秘密パラメータと、前記記録媒体との間で交換される第4の公開パラメータとに基づき第5の鍵情報を生成する第4の鍵生成手段と、この第4の鍵生成手段で生成された第5の鍵情報を用いて前記第2の受信手段で受信された暗号化された識別情報を復号する第3の復号手段と、前記判定手段は、この第3の復号手段で復号された識別情報と前記復号されたライセンス情報とに基づき前記コンテンツ情報の利用の可否を判定することを特徴とする請求項61記載の判定装置。

【請求項66】 少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報を復号および利用する情報利用装置において、前記ライセンス情報の配信装置との間で共有される第1の秘密パラメータを記憶する第1の記憶手段と、この第1の記憶手段に記憶された第1の秘密パラメータと前記配信装置との間で交換される第1の公開パラメータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、受信した前記暗号化されたライセンス情報を前記第1の鍵生成手段で生成された第2の鍵情報で復号する第1の復号手段と、この第1の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第1の鍵情報を用いて前記コンテンツ情報を復号することを特徴とする情報利用装置。

【請求項67】 前記ライセンス情報に含まれる、少なくとも前記第1の鍵情報と前記利用条件とを含む暗号化された第1の暗号情報を復号する第3の鍵情報を記憶する第2の記憶手段と、前記復号手段で復号されたライセンス情報に含まれる前記第1の暗号情報を前記第2の記憶手段に記憶されている第3の鍵情報を用いて復号する第2の復号手段と、を具備したことを特徴とする請求項66記載の情報利用装置。

【請求項68】 前記配信装置との間の通信は、演算機能を有する記録媒体を介して行われることを特徴とする

請求項66記載の情報利用装置。

【請求項69】 前記配信装置との間の通信は、演算機能を有する記録媒体を介して行われ、前記該記録媒体との間で共有される第2の秘密パラメータを記憶する第3の記憶手段と、前記記録媒体から該記録媒体の暗号化された識別情報を受信する受信手段と、前記第3の記憶手段に記憶された第2の秘密パラメータと、前記記録媒体との間で交換される第2の公開パラメータとに基づき第4の鍵情報を生成する第4の鍵生成手段と、前記受信手段で受信された暗号化された識別情報を前記第4の鍵生成手段で生成された第4の鍵情報を用いて復号する第3の復号手段と、前記判定手段は、この第3の復号手段で復号された識別情報と前記復号されたライセンス情報とに基づき前記コンテンツ情報の利用の可否を判定することを特徴とする請求項66記載の情報利用装置。

【請求項70】 少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報とが記録された演算機能を有する記録媒体であって、前記ライセンス情報の記録装置との間で共有される第1の秘密パラメータと、前記ライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置との間で共有される第2の秘密パラメータとを記憶する第1の記憶手段と、予め与えられた識別情報を記憶する第2の記憶手段と、前記第1の記憶手段に記憶された第1の秘密パラメータと前記記録装置との間で交換される第1の公開パラメータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、この第1の鍵生成手段で生成された第2の鍵情報を用いて前記識別情報を暗号化する第1の暗号手段と、前記第1の記憶手段に記憶された第2の秘密パラメータと前記判定装置との間で交換される第2の公開パラメータとに基づき第3の鍵情報を生成する第2の鍵生成手段と、この第2の鍵生成手段で生成された第3の鍵情報を用いて前記識別情報を暗号化する第2の暗号手段と、前記第1および第2の暗号手段で暗号化された識別情報を前記記録装置および前記判定装置に送信する送信手段と、を具備したことを特徴とする記録媒体。

【請求項71】 少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報が記録された演算機能を有する記録媒体であって、前記ライセンス情報の記録装置との間で共有される第1の秘密パラメータと、前記ライセンス情報に基づき前記



コンテンツ情報を利用する情報利用装置との間で共有される第2の秘密パラメータとを記憶する第1の記憶手段と、

予め与えられた識別情報を記憶する第2の記憶手段と、前記第1の記憶手段に記憶された第1の秘密パラメータと前記記録装置との間で交換される第1の公開パラメータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、

この第1の鍵生成手段で生成された第1の鍵情報を用いて前記識別情報を暗号化する第1の暗号手段と、前記第1の記憶手段に記憶された第2の秘密パラメータと前記情報利用装置との間で交換される第2の公開パラメータとに基づき第3の鍵情報を生成する第2の鍵生成手段と、

この第2の鍵生成手段で生成された第3の鍵情報を用いて前記識別情報を暗号化する第2の暗号手段と、前記第1および第2の暗号手段で暗号化された識別情報を前記記録装置および前記情報利用装置に送信する送信手段と、

を具備したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばDVD等の記録媒体に記録された、あるいは、ネットワークを介して、あるいは放送にて分配された情報の利用に対して課金を行う情報記録／再生装置を含む情報流通システムに関する。

【0002】特に、例えばDVD等の記録媒体に情報を記録する情報記録装置およびDVD等の記録媒体に記録された情報を再生する情報再生装置に関する。

【0003】

【従来の技術】近年、デジタル情報処理技術や広帯域ISDN等の通信技術の発達、DVD等の大容量、高画質、高音質を実現する高度な情報記録媒体の開発が進んでいる。このような情報の伝達手段の多様化、高度化が進むにつれ、デジタル化された著作物等がネットワーク、記録媒体などを介して利用者の手元に大量に頒布され、利用者がそれらを自由に利用できる環境が生まれつつある。このような環境は、著作物の無断複製、無断改変、著作者の意図しない流通などが起こる機会を増大させるものであり、著作物の権利者にとって、自己の利益が不当に害されるのではないかという懸念を抱かせるものである。

【0004】このような著作物の権利者の懸念を拭い払えるよう、迅速かつ手軽にデジタル化された著作物を流通させるとともに、適正にそれらを利用できるようなデジタル情報の利用環境を提供できる著作権の保護を前提としたシステムの開発は今後の重要な課題となる。

【0005】DVDは、CD-ROMに代わる大容量のパソコンメディアであるとともに、映画、音楽、ゲー

ム、カラオケ等、様々な用途への広がり期待でき、このようなDVDの普及を図るために、DVDのタイトル価格を低く抑えたり、レンタルDVD市場への拡大も予想される。従って、このような観点からも、DVD等の記録媒体に記録されたデジタル化された著作物の所有ではなく利用に対して課金するという考えに基づく、情報に対する著作権の保護を前提とした情報の流通システムが不可欠となる。

【0006】

【発明が解決しようとする課題】そこで、本発明は、デジタル化された著作物を迅速かつ手軽に流通させるとともに、著作権の保護を前提としたデジタル情報の利用環境を提供する情報流通システムを構築するための情報記録装置および情報再生装置および課金装置を提供することを目的とする。すなわち、ネットワークあるいは記録媒体を介して分配されたデジタル化された著作物を迅速かつ手軽に流通させるとともに、デジタル情報の利用に対する課金による著作権の保護を前提としたデジタル情報の利用環境を構築するための情報記録装置およびその記録された情報の再生装置および情報利用に対する課金装置を提供することを目的とする。

【0007】

【課題を解決するための手段】（第1の実施形態）

（1）本発明の情報記録装置（請求項1）は、コンテンツ情報を暗号化する暗号化手段と、少なくとも前記コンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号する復号鍵とを含む暗号化されたライセンス情報を生成するライセンス情報生成手段と、前記暗号化手段で暗号化されたコンテンツ情報と前記ライセンス情報生成手段で生成されたライセンス情報とを記録媒体に記録する記録手段と、を具備する。

【0008】また、本発明の情報再生装置（請求項4）

は、暗号化されたコンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件および前記コンテンツ情報を復号するための第1の鍵情報を含む暗号化されたライセンス情報とが記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、前記ライセンス情報を復号するための第2の鍵情報を記憶する記憶手段と、この記憶手段に記憶されている第2の鍵情報を用いて前記記録媒体に記録されているライセンス情報を復号する第1の復号手段と、この第1の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記第1の復号手段で復号されたライセンス情報に含まれる第1の鍵情報を用いて前記記録媒体に記録されているコンテンツ情報を復号する第2の復号手段と、を具備する。

【0009】本発明の情報記録装置により、暗号化されたコンテンツ情報と該コンテンツ情報の利用条件が不可



分になるよう記録媒体に記録される。このような記録媒体に記録されたコンテンツ情報を再生するには、ライセンス情報を復号するための正当な復号鍵を具備した情報再生装置のみが行え、しかも復号の際には、必ずライセンス情報に含まれる利用条件を参照してコンテンツ情報の利用の可否を判断するため、コンテンツ情報を不正な利用条件の下で利用する事が不可能となる。従って、該コンテンツ情報の著作権の保護を前提としたデジタル情報を迅速かつ手軽に流通させることができる。

【0010】(2) また、本発明の情報記録装置(請求項2)は、コンテンツ情報から一部の情報を分離する分離手段と、少なくとも、前記分離手段で分離された前記一部の情報と前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化されたライセンス情報を生成するライセンス情報生成手段と、このライセンス情報生成手段で生成されたライセンス情報と前記コンテンツ情報の他の一部を記録媒体に記録する記録手段と、を具備する。

【0011】本発明の情報再生装置(請求項5)は、コンテンツ情報の一部と、少なくとも前記コンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報の他の一部を含む暗号化されたライセンス情報とが記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、前記ライセンス情報を復号する鍵情報を記憶する記憶手段と、この記憶手段に記憶されている鍵情報を用いて前記記録媒体に記録されているライセンス情報を復号する復号手段と、この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる前記コンテンツ情報の一部と、前記記録媒体に記録されている前記コンテンツ情報の一部とを合成して前記コンテンツ情報を再生する再生手段と、を具備する。

【0012】本発明の情報記録装置により、コンテンツ情報と該コンテンツ情報の利用条件が不可分になるよう記録媒体に記録される。このような記録媒体に記録されたコンテンツ情報を再生するには、ライセンス情報を復号するための正当な復号鍵を具備した情報再生装置のみが行え、しかも復号の際には、必ずライセンス情報に含まれる利用条件を参照してコンテンツ情報の利用の可否を判断するため、コンテンツ情報を不正な利用条件の下で利用する事が不可能となる。従って、該コンテンツ情報の著作権の保護を前提としたデジタル情報を迅速かつ手軽に流通させることができる。

【0013】(3) 本発明の情報記録装置(請求項3)は、コンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化された記録情報を生成する記録情報生成手段と、この記録情報生成手段で生成された記録情報を記録媒体に記録す

る記録手段と、を具備する。

【0014】本発明の情報再生装置(請求項6)は、少なくともコンテンツ情報と前記コンテンツ情報の利用を制限するための利用条件とを含む暗号化された記録情報が記録された記録媒体から前記コンテンツ情報を再生する情報再生装置において、前記記録情報を復号するための鍵情報を記憶する記憶手段と、この記憶手段に記憶されている鍵情報を用いて前記記録媒体に記録されている記録情報を復号する復号手段と、この復号手段で復号された記録情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたコンテンツ情報を再生する再生手段と、を具備する。

【0015】本発明の情報記録装置により、コンテンツ情報と該コンテンツ情報の利用条件が不可分になるよう記録媒体に記録される。このような記録媒体に記録されたコンテンツ情報を再生するには、記録情報を復号するための正当な復号鍵を具備した情報再生装置のみが行え、しかも復号の際には、必ず利用条件を参照してコンテンツ情報の利用の可否を判断するため、コンテンツ情報を不正な利用条件の下で利用する事が不可能となる。従って、該コンテンツ情報の著作権の保護を前提としたデジタル情報を迅速かつ手軽に流通させることができる。

【0016】(4) 本発明の課金装置(請求項15)は、記録媒体に記録されたコンテンツ情報の利用に対する課金を行う課金装置において、記録媒体に記録されたコンテンツ情報の利用条件を入力する入力手段と、この入力手段で入力された利用条件に基づき前記コンテンツ情報の利用に対する料金の支払いを要求する要求手段と、前記要求に応じて料金の支払いが確認されたとき、少なくとも前記入力手段で入力された利用条件を含むライセンス情報を前記記録媒体に記録する記録手段と、を具備することにより、コンテンツ情報およびその利用を制限する利用条件を含むライセンス情報の記録された記録媒体に対し、該コンテンツ情報の利用に対する適切な課金が行えるとともに、該コンテンツ情報の著作権の保護を前提としたデジタル情報を迅速かつ手軽に流通させることができる。

【0017】(5) 本発明の課金装置(請求項16)は、コンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件を含む暗号化されたライセンス情報とが記録された記録媒体を介した前記コンテンツ情報の利用に対する課金を行う課金装置において、前記記録媒体に記録された暗号化されたライセンス情報を入力する入力手段と、この入力手段で入力された暗号化されたライセンス情報を復号する復号手段と、前記コンテンツ情報を利用するための利用条件を入力する利用条件入力手段と、この利用条件入力手段で入力さ

れた利用条件に基づき前記コンテンツ情報の利用に対する料金の支払いを要求する要求手段と、前記要求に応じて料金の支払いが確認されたとき、前記利用条件入力手段で入力された利用条件に基づき前記復号手段で復号されたライセンス情報を更新する更新手段と、この更新手段で更新されたライセンス情報を暗号化する暗号手段と、この暗号手段で暗号化されたライセンス情報を出力する出力手段と、を具備することにより、コンテンツ情報およびその利用を制限する使用条件を含むライセンス情報の記録された記録媒体に対し、該コンテンツ情報の利用に対する適切な課金が行えるとともに、該コンテンツ情報の著作権の保護を前提としたデジタル情報を迅速かつ手軽に流通させることができる。

(第2の実施形態)

(6) 本発明の判定装置(請求項17、請求項18、請求項49:復号ユニットA)は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、前記ライセンス情報を復号する第2の鍵情報を予め定められた時間毎に生成する鍵生成手段と、入力された前記ライセンス情報を前記鍵生成手段で生成された第2の鍵情報を用いて復号する復号手段と、この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第1の鍵情報を出力する出力手段と、を具備する。

【0018】本発明によれば、ライセンス情報を復号するための秘密鍵(第2の鍵情報)を復号ユニットA内で所定タイミング毎に生成し、これをある所定期間に限って用いるようになっているため、コンテンツ情報の利用条件やコンテンツ情報の復号鍵を含むライセンス情報の情報セキュリティの向上が図れる。

【0019】(7) 本発明の判定装置(請求項19、請求項20:復号ユニットB)は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第1の鍵情報と該暗号化された第1の鍵情報を復号するための第2の鍵情報を生成するために必要な第1の鍵生成情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、前記ライセンス情報を復号する復号手段と、この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる暗号化された第1の鍵情報と第1の鍵生成情報とを出力する出力手段と、を具備する。

【0020】本発明によれば、コンテンツ情報を復号する第1の鍵情報は、復号ユニットB内では暗号化されたままなので、コンテンツ情報の復号鍵情報の情報セキュリティの向上が図れる。

【0021】(8) 本発明の判定装置(請求項21、請求項22、請求項50:復号ユニットC)は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための暗号化された第1の鍵情報と該暗号化された第1の鍵情報を復号するための第2の鍵情報を生成するために必要な第1の鍵生成情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、前記ライセンス情報を復号する第3の鍵情報を予め定められた時間毎に生成する鍵生成手段と、入力された前記ライセンス情報を前記鍵生成手段で生成された第3の鍵情報を用いて復号する復号手段と、この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる暗号化された第1の鍵情報と第1の鍵生成情報とを出力する出力手段と、を具備する。

【0022】本発明によれば、ライセンス情報を復号するための秘密鍵(第3の鍵情報)を復号ユニットC内で所定タイミング毎に生成し、これを所定期間に限って用いるようになっているため、コンテンツ情報の利用条件やコンテンツ情報の復号鍵を含むライセンス情報の情報セキュリティの向上が図れる。また、コンテンツ情報を復号する第1の鍵情報は、復号ユニットC内では暗号化されたままなので、復号鍵情報の情報セキュリティの向上が図れる。

【0023】(9) 本発明の判定装置(請求項23、請求項24:復号ユニットD、復号ユニットD')は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを第2の鍵情報で暗号化したものと、少なくとも該第2の鍵情報を生成するために必要な鍵生成情報とを含むライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置において、入力された前記ライセンス情報に含まれる鍵生成情報に基づき前記第2の鍵情報を生成する鍵生成手段と、この鍵生成手段で生成された第2の鍵情報を用いて前記ライセンス情報に含まれる利用条件と第1の鍵情報とを復号する復号手段と、この復号手段で復号された利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号された第1の鍵情報を出力する出力手段と、を具備する。

【0024】本発明によれば、ライセンス情報の暗号化部分(セキュリティ対策を要する重要な情報部分)を復

号する第1の鍵情報は、該暗号化部分を復号する際に、その都度生成され、復号後はメモリ上から消去できるため、復号ユニットD、D'内に該第1の鍵情報を保持することがない。従って、利用条件やコンテンツ情報を復号する第1の鍵情報等の重要な情報（第三者には知られて不正利用されては困るような情報）のセキュリティの向上が図れる。

【0025】また、ライセンス情報が更新される度に第1の鍵情報（ $K_{AB}$ ）が異なるので、第1の鍵情報が露見した場合の影響が少なくなる。そればかりか公開鍵暗号に比べ格段に高速である共有鍵暗号が使えるので付加情報のデータサイズを大きくしても実時間で復号し、ライセンス情報に含まれる利用条件に基づくコンテンツの利用可否の反映が行えるという利点がある。

【0026】（10） 本発明の更新装置（請求項25：復号ユニットAに対応するライセンス情報更新装置）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための鍵情報とを含む公開鍵で暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と更新された公開鍵とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、前記更新されたライセンス情報を前記通知された公開鍵で暗号化することを特徴とする。

【0027】本発明によれば、ライセンス情報の更新の際には、コンテンツ復号鍵を通知する必要がなく、情報セキュリティの確保されたライセンス情報の更新が可能となる。

【0028】（11） 本発明の更新装置（請求項26：復号ユニットBに対応するライセンス情報更新装置）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第1の鍵情報と該暗号化された第1の鍵情報を復号する第2の鍵情報を生成するために必要な第1の鍵生成情報とを含む暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と前記第2の鍵情報を生成するために必要な第2の鍵生成情報とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、前記利用条件と前記第1の鍵生成情報とを更新し、該更新された第1の鍵生成情報と前記第2の鍵生成情報とに基づき前記第2の鍵情報を更新し、この更新された第2の鍵情報で前記第1の鍵情報を暗号化して、少なくとも該更新された利用条件と該更新された第2の鍵情報で暗号化された第1の鍵情報と該更新された第1の鍵生成情報とを含む暗号化されたライセンス情報を生成することを特徴とする。

【0029】本発明によれば、ライセンス情報の更新の際には、コンテンツ復号鍵を通知する必要がなく、情報セキュリティの確保されたライセンス情報の更新が可能となる。

【0030】（12） 本発明の更新装置（請求項27：復号ユニットCに対応するライセンス情報更新装置）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための暗号化された第1の鍵情報と該暗号化された第1の鍵情報を復号する第2の鍵情報を生成するために必要な第1の鍵生成情報とを含む公開鍵で暗号化されたライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも新たに指定された利用条件と前記第2の鍵情報を生成するために必要な第2の鍵生成情報と更新された公開鍵とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、前記利用条件と前記第1の鍵生成情報とを更新し、該更新された第1の鍵生成情報と前記第2の鍵生成情報とに基づき前記第2の鍵情報を更新し、この更新された第2の鍵情報で前記第1の鍵情報を暗号化して、少なくとも該更新された利用条件と該更新された第2の鍵情報で暗号化された第1の鍵情報と該更新された第1の鍵生成情報とを含むライセンス情報を生成し、この生成されたライセンス情報を前記通知された公開鍵で暗号化することを特徴とする。

【0031】本発明によれば、ライセンス情報の更新の際には、コンテンツ復号鍵を通知する必要がなく、情報セキュリティの確保されたライセンス情報の更新が可能となる。

【0032】（13） 本発明の更新装置（請求項28：復号ユニットD、D'に対応するライセンス情報更新装置）は、少なくともコンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための第1の鍵情報とを第2の鍵情報で暗号化したものと、少なくとも該第2の鍵情報を生成するために必要な2つの鍵生成情報とを含むライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置から、少なくとも前記2つの鍵生成情報のうちの一方あるいは該一方の鍵生成情報を更新したものと新たに指定された利用条件とが通知されて前記ライセンス情報の更新の要求を受けたとき、該要求に基づき該ライセンス情報を更新する更新装置であって、前記利用条件と他方の鍵生成情報とを更新し、該更新された他方の鍵生成情報と前記通知された一方の鍵生成情報とに基づき前記第2の鍵情報を更新して、少なくとも該更新された利用条件と該第1の鍵情報とを該更新された第2の鍵情報で暗号化したものと、少なくとも前記通知された一方の鍵生成情報と該更新された他方の鍵生成情報とを含むライセンス情報を生成することを特徴とする。

【0033】本発明によれば、ライセンス情報の更新の際には、コンテンツ復号鍵を通知する必要がなく、情報セキュリティの確保されたライセンス情報の更新が可能となる。

【0034】(14) 本発明の情報利用装置(請求項29: 復号ユニットB、Cに対応する情報利用装置)は、暗号化されたコンテンツ情報を復号するための暗号化された第1の鍵情報と該第1の鍵情報を復号する第2の鍵情報を生成するために必要な第1の鍵生成情報とが入力されて、該コンテンツ情報を復号および利用する情報利用装置において、前記第1の鍵情報を復号する第2の鍵情報を生成するために必要な第2の鍵生成情報を保持し、この第2の鍵生成情報と前記入力された第1の鍵生成情報とに基づき前記第2の鍵情報を生成し、この生成された第2の鍵情報を用いて前記暗号化されたコンテンツ情報を復号することを特徴とする。

【0035】本発明によれば、コンテンツ情報の復号鍵(第1の鍵情報)は暗号化されたまま当該情報利用装置に入力するため、第1の鍵情報を出力する装置(復号ユニットB、C)と当該情報利用装置との間における情報セキュリティの向上が図れる。

(第3の実施形態)

(15) 本発明の情報利用装置(請求項30)は、記録媒体に記録された暗号化されたコンテンツ情報を該記録媒体に記憶された、少なくとも前記コンテンツ情報の利用を制限するための利用条件と前記コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき復号および利用する情報利用装置において、日時を計測する計測手段と、この計測手段で計測された日時と前記記録媒体に記録されたライセンス情報とに基づき前記コンテンツ情報の利用の可否を判定する判定手段と、前記判定手段で前記コンテンツ情報の利用が可能と判定されたとき該判定手段から出力される前記第1の鍵情報を用いて前記記録媒体に記録されたコンテンツ情報を復号する復号手段と、を具備し、前記計測手段から前記判定手段へ日時を通知するための情報と、前記判定手段から前記復号手段へ出力される第1の鍵情報とは暗号化されていることを特徴とする。

【0036】本発明によれば、情報生成装置内の各機能ユニット(計測手段、判定手段、復号手段)間で受け渡される情報のセキュリティの向上が図れる。

【0037】(16) 本発明の判定装置(請求項42)は、暗号化されたコンテンツ情報と、少なくとも前記コンテンツ情報の利用を制限するための利用条件および前記コンテンツ情報を復号するための第1の鍵情報を含む暗号化されたライセンス情報とが記録された記録媒体から読み出された該暗号化されたライセンス情報と、日時を通知するための暗号化された日時情報とを入力して、前記コンテンツ情報の利用の可否を判定する判定装置であって、前記暗号化されたライセンス情報を復号す

る第1の復号手段と、前記暗号化された日時情報を復号する第2の復号手段と、前記第1および第2の復号手段で復号された情報に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき前記第1の鍵情報を暗号化して出力する出力手段と、を具備し、演算機能を有する携帯可能記録媒体で構成されたことを特徴とする。

【0038】本発明の判定装置を例えばパーソナルコンピュータに装着して用いた場合、当該判定装置に入力あるいは出力される情報のセキュリティの向上が図れる。

(第4の実施形態)

(17) (請求項51) 請求項17、19、21、23、24記載の判定装置において、前記復号手段で復号された前記ライセンス情報には、復号結果の正否を判定するための認証情報が含まれていることにより、時間の経過に従って該ライセンス情報の復号化鍵がいくつも生成される状況であっても、そのうちのいずれか正しい復号鍵で当該ライセンス情報が復号されたか否かを容易に判断できる。

【0039】(18) 本発明の判定装置(請求項52)は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、前記ライセンス情報を復号する第2の鍵情報を放送配信される第1の鍵生成情報に基づき生成する鍵生成手段と、入力された前記ライセンス情報を前記鍵生成手段で生成された第2の鍵情報を用いて復号する復号手段と、この復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第1の鍵情報を出力する出力手段と、を具備したことにより、暗号化ライセンス情報の復号化鍵(第2の鍵情報)を生成するために必要なシード情報(第1の鍵生成情報)が放送配信されるので、暗号化ライセンス情報の復号化鍵の更新が容易に行える。

(第5の実施形態)

(19) 本発明の鍵配信装置(請求項55)は、記録媒体に記録された暗号化されたコンテンツ情報を復号するために必要な第1の鍵情報を前記コンテンツ情報を利用する情報利用装置へ配信する鍵配信装置において、前記情報利用装置との間で共有される第1の秘密パラメータを記憶する第1の記憶手段と、この第1の記憶手段に記憶された第1の秘密パラメータと、該情報利用装置との間で交換される第1の公開パラメータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、少なくとも前記第1の鍵情報を含む暗号化された第1の暗号情報を、前

記第1の鍵生成手段で生成された第2の鍵情報で暗号化する暗号手段と、この暗号手段で暗号化された少なくとも前記第1の暗号情報を含む第2の暗号情報を前記情報利用装置に配信する配信手段と、を具備したことにより、コンテンツ情報を復号するために必要なディスクキー（第1の鍵情報）を、その配信元（鍵配信装置としてのライセンス作成装置、ライセンス注入装置）から配信先（情報利用装置としてのカードアダプタ、プレーヤ）とで、双方で共有する秘密パラメータから生成される公開してもかまわない公開パラメータを伝達し合い、自分の秘密パラメータと相手からの公開パラメータによって鍵配送を達成するので、盗聴されるかもしれない安全でない通信路であっても安全に鍵配信が行える。

【0040】（20）本発明の判定装置（請求項61）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報の利用の可否を判定する判定装置において、前記ライセンス情報の配信装置との間で共有される第1の秘密パラメータを記憶する第1の記憶手段と、この第1の記憶手段に記憶された第1の秘密パラメータと前記配信装置との間で交換される第1の公開パラメータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、受信した前記暗号化されたライセンス情報を前記第1の鍵生成手段で生成された第2の鍵情報で復号する第1の復号手段と、この第1の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第1の鍵情報を出力する出力手段と、を具備したことにより、コンテンツ情報を復号するために必要なディスクキー（第1の鍵情報）の配信元（配信装置としてのライセンス作成装置、ライセンス注入装置）との間で共有する秘密パラメータから生成される公開してもかまわない公開パラメータを伝達し合い、自分の秘密パラメータと配信元からの公開パラメータによって鍵配送を達成するので、盗聴されるかもしれない安全でない通信路であっても安全に第1の鍵情報を受け取れる。

【0041】（21）本発明の情報利用装置（請求項66）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報に基づき、前記コンテンツ情報を復号および利用する情報利用装置において、前記ライセンス情報の配信装置との間で共有される第1の秘密パラメータを記憶する第1の記憶手段と、この第1の記憶手段に記憶された第1の秘密パラメータと前記配信装置との間で交換される第1の公開パラメータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、受信した前記暗号化されたライセンス情報

を前記第1の鍵生成手段で生成された第2の鍵情報で復号する第1の復号手段と、この第1の復号手段で復号されたライセンス情報に含まれる利用条件に基づき前記コンテンツ情報の利用の可否を判定する判定手段と、この判定手段で前記コンテンツ情報の利用が可能と判定されたとき、前記復号手段で復号されたライセンス情報に含まれる第1の鍵情報を用いて前記コンテンツ情報を復号することを特徴とする。

【0042】本発明によれば、コンテンツ情報を復号するために必要なディスクキー（第1の鍵情報）の配信元（配信装置としてのライセンス作成装置、ライセンス注入装置）との間で共有する秘密パラメータから生成される公開してもかまわない公開パラメータを伝達し合い、自分の秘密パラメータと配信元からの公開パラメータによって鍵配送を達成するので、盗聴されるかもしれない安全でない通信路であっても安全に第1の鍵情報を受け取れる。

【0043】（22）本発明の記録媒体（請求項70、71）は、少なくともコンテンツ情報の利用を制限するための利用条件と該コンテンツ情報を復号するための第1の鍵情報とを含む暗号化されたライセンス情報とが記録された演算機能を有する記録媒体であって、前記ライセンス情報の記録装置との間で共有される第1の秘密パラメータと、前記ライセンス情報に基づき前記コンテンツ情報の利用の可否を判定する判定装置（あるいは、前記コンテンツ情報を利用する情報利用装置）との間で共有される第2の秘密パラメータとを記憶する第1の記憶手段と、予め与えられた識別情報を記憶する第2の記憶手段と、前記第1の記憶手段に記憶された第1の秘密パラメータと前記記録装置との間で交換される第1の公開パラメータとに基づき第2の鍵情報を生成する第1の鍵生成手段と、この第1の鍵生成手段で生成された第2の鍵情報を用いて前記識別情報を暗号化する第1の暗号手段と、前記第1の記憶手段に記憶された第2の秘密パラメータと前記判定装置（あるいは前記情報利用装置）との間で交換される第2の公開パラメータとに基づき第3の鍵情報を生成する第2の鍵生成手段と、この第2の鍵生成手段で生成された第3の鍵情報を用いて前記識別情報を暗号化する第2の暗号手段と、前記第1および第2の暗号手段で暗号化された識別情報を前記記録装置および前記判定装置（あるいは前記情報利用装置）に送信する送信手段と、を具備したことにより、コンテンツ情報を復号するために必要なディスクキー（第1の鍵情報）を、その配信元（記録装置としてのライセンス注入装置）から配信先（判定装置（あるいは情報利用装置）としてのカードアダプタ、プレーヤ）へ配信する記録媒体が、その識別情報を当該配信元および配信先のそれぞれとの間で共有する秘密パラメータから生成される公開してもかまわない公開パラメータを伝達し合い、自分の秘密パラメータと相手からの公開パラメータによっ

て配送するので、盗聴されるかもしれない安全でない通信路であっても安全に当該識別情報の配信が行えるとともに、当該識別情報を有する記録媒体のみがディスクキーを配信するための正当な記録媒体であることを配信元および配信先との間で認識できるので（例えば、配信元にてライセンス情報に当該記録媒体の識別情報を含めることにより、配信先にて、このライセンス情報に含まれる識別情報と、当該ライセンス情報の記録されていた記録媒体の識別情報とが一致していたときにライセンス判定を行う）、当該記録媒体を介して双方でディスクキーが安全に受け渡しできる。

【0044】

【発明の実施の形態】以下、本発明の実施形態について図面を参照して説明する。

（第1の実施形態）まず、本発明の第1の実施形態に係る情報記録装置および情報再生装置を用いた情報流通システムの全体を概略的に説明する。

【0045】本発明に係る情報記録装置および情報再生装置を用いた情報流通システムの構成例を図53に示す。図53において、ライセンス情報生成部1002、情報記録部1003は、図1、図3、図7等に示したライセンス情報生成部および情報記録部と等価であり、復号ユニット1013は、図9、図12、図27、図39、図43等に示す復号ユニットと等価である。再生部1014、読み出し部1012も、図8等に示す情報再生装置の再生部、読み出し部と等価である。

【0046】図53に示すシステム全体の動作を以下、簡単に説明する。課金対象情報は暗号鍵 $k_e(1)$ によって暗号化されている（「課金対象情報」 $k_e(1)$ ）。まず、ライセンス情報生成部1002に課金対象情報の復号鍵 $k_d(1)$ と利用期限等の利用条件が入力される（ステップS701、ステップS702）。

【0047】ライセンス情報生成部1002は複合鍵 $k_d(1)$ と利用条件とをマージした後、暗号鍵 $k_e$ によって暗号化してライセンス情報を生成し、それを情報記録部1003に送る（ステップS703）。一方、暗号化された課金対象情報も情報記録部1003に入力され（ステップS704）、ライセンス情報と共に情報蓄積部1004に記録される（ステップS705）。

【0048】情報蓄積部1004は、DVD-ROMやDVD-RAM、ハードディスク等のメディアである。このメディアに記録された情報が直に、或いは放送やインターネット等を通じて別のメディア（すなわち、情報蓄積部1015）に移し替えられて、情報再生装置1011の読み出し部1012によって読み出される（ステップS706）。読み出されたライセンス情報は、復号ユニット1013に送られる（ステップS707）。復号ユニット1013は、暗号鍵 $k_e$ に対する復号鍵 $k_d$ を保持しており、ライセンス情報を復号し、課金対象情報の復号鍵 $k_d(1)$ と利用条件とを取り出す。復号ユ

ニット1013は利用条件をチェックし、課金対象情報が利用可能か否かを決定する。利用可能であれば、復号ユニットは復号鍵 $k_d(1)$ を、再生部1014に対して出力する（ステップS708）。再生部1014は、読み出し部1012から「課金対象情報」 $k_e(1)$ を取り出し（ステップS709）、復号鍵 $k_d(1)$ によって復号し、課金対象情報を再生する。

【0049】復号ユニット1013は、復号鍵 $k_d$ と、ライセンス情報の復号を行うアルゴリズムとを保持している。セキュリティに対する攻撃を避ける為に、復号ユニット1013は、ソフトウェアではなく、例えばICチップとして実装する事が望ましい。この場合、復号ユニット1013はライセンス情報の入力部と、（利用可能と判断した場合に）課金対象情報の復号鍵を出力する出力部を具備したICチップであり、復号や利用可否の判断は全てチップ内で行われる。

【0050】本発明の要点の1つは、ライセンス情報生成部1002が、課金対象情報の復号鍵 $k_d(1)$ と利用条件とをマージした後、暗号化を施す点にある。一般に暗号化は、暗号化対象情報のビットを攪拌する。従って、暗号化処理後は、同時に暗号化された2つの情報を分離する事は（復号による他は）不可能になる。暗号化処理のこの性質を利用して、課金対象情報と利用条件とを分離不可能にする事が重要である。

【0051】以上説明した実施形態の場合、課金対象情報は暗号鍵 $k_e(1)$ によって暗号化されている。従って、

1. 課金対象情報を利用するためには、復号鍵 $k_d(1)$ を要する。ところが、復号鍵 $k_d(1)$ は、ライセンス情報の一部として、利用条件と不可分に暗号化されている。ライセンス情報と課金対象情報とは分離可能であるが、適正でないライセンス情報は、課金対象情報を正しく復号するための復号鍵を含まないの、ライセンス情報の「すり替え」は意味をなさない。

【0052】2. 正しい復号鍵 $k_d(1)$ を得る為には、適正なライセンス情報を復号しなければならない。ところが、

3. この復号は復号鍵 $k_e$ を保持する正統的な復号ユニットによってしか、行い得ない。そして、

4. 正統的な復号ユニットは、ライセンス情報に含まれる利用条件を必ず参照し、利用の可否を判定する。従って、

5. 本発明のライセンス情報生成部および復号ユニットを含む装置においては、課金対象情報を不正な利用条件の下で利用する事が原理的に不可能である。

【0053】復号ユニット1013が、課金対象情報を利用不可と判定し、復号鍵 $k_d(1)$ の出力を行わなかった場合、課金対象情報を利用する為には、ライセンス情報の更新又は有効なライセンス情報の追加を行う他はない。この時点が、情報利用者に対する課金発生タイ

ミングである。利用者は、店舗や自動販売機、或いはインターネット経由等、何らかの方法でライセンス情報の更新又は新規取得を行わなければならない。店舗に設置された装置や自動販売機、或いはネットワーク・サーバーは、復号鍵k dと暗号化の鍵k eを保持しており、ライセンス情報の復号と情報の書き換え及び再暗号化を行い、ライセンス情報を更新する事ができる。

【0054】利用者がライセンス情報の更新（又は新規発行）を受ける為には、当該課金対象情報に付帯するライセンス情報（の1つ）を、ライセンス情報更新機能を有する装置に送らなければならない。

【0055】1' . 復号鍵k dと暗号化用の鍵k eとを有する正統的な装置のみが、課金対象情報の復号鍵k d（1）と利用条件とを復号・分離する事が可能であり、

2' . 復号鍵k dと暗号化用の鍵k eとを有する正統的な装置のみが、利用条件を書き換えた後ライセンス情報として再暗号化する事が出来る。

【0056】更新されたライセンス情報は、ライセンス情報更新装置（図26ライセンス情報更新クライアント部403、図38のライセンス情報更新ユニット603、図41のライセンス情報更新ユニット702、図47のライセンス情報更新ユニット804）から出て、利用者の所有するメディアに書き戻される。ライセンス情報更新装置の内部以外の場所では、ライセンス情報は暗号化された状態のままであり、

3' . 本発明に特徴的な暗号化を施されている為、利用条件に対して不正な変更を施す事が不可能である。

【0057】一般に、復号用の鍵をネットワークを通じて送信する為に、別の鍵を用いて再び暗号化する等と言う事は、しばしば行われている。しかし、暗号化された課金対象情報を復号する鍵k d（1）と利用条件とをマージした後に暗号化するという、本発明の特徴は、著作物等の課金対象情報の保護と課金において、上述の様に大きな効果を発揮するものである。

【0058】以下、本発明の情報記録装置および情報再生装置および課金装置の構成および動作について、詳細に説明する。

#### （1）情報記録装置

##### （1-1）情報記録装置の第1の例

図1は、本発明に係る情報記録装置の第1の構成例を示したものである。すなわち、図1は、デジタル化された著作物等の課金対象であるコンテンツ情報（以下、課金対象情報と呼ぶ）を暗号化し、その課金対象情報の利用条件と暗号化された課金対象情報を復号するための復号鍵とを暗号化してライセンス情報を生成し、暗号化された課金対象情報およびライセンス情報を所定の記録媒体に記録する情報記録装置の構成例を示したものである。

【0059】情報記録装置は、大きく分けて課金対象情

報入力部2、ライセンス情報生成部3、記録部8から構成される。

【0060】課金対象情報は、暗号鍵k e（1）を用いて予め暗号化されていて、課金対象情報入力部2に入力される。なお、暗号鍵k e（1）に対応する復号鍵をk d（1）とする。今後、情報Xが暗号鍵Kによって暗号化されている事を[X]kと表現することがある。

【0061】ライセンス情報生成部3は、利用条件入力部4、復号鍵入力部5、鍵保持部6、暗号化部7から構成される。

【0062】鍵保持部6には、暗号鍵k eが予め記憶されている。この暗号鍵k eは、必ずしもk e（1）とは一致しない。

【0063】利用条件入力部4には、利用条件が入力する。利用条件とは、課金対象情報の利用期限、ライセンス情報書き込み時刻、コンテンツID、メディアIDあるいは復号ユニットIDのうちの少なくとも1つから構成されている。

【0064】復号鍵入力部5には、暗号化された課金対象情報を復号するための暗号鍵k e（1）に対応する復号鍵k d（1）が入力する。

【0065】暗号化部7には、利用条件入力部4、復号鍵入力部5を介して、利用条件、復号鍵k d（1）がそれぞれ入力し、利用条件と復号鍵k d（1）がマージされる。その後、鍵保持部6に記憶されている暗号鍵k eを用いてマージされた利用条件と復号鍵k d（1）を暗号化する。暗号化の方式としては、一般的に、大きく分けて公開鍵方式と秘密鍵方式があるが、いずれを採用しても良い。ここで暗号化を施されたデータをライセンス情報と呼ぶ。暗号化部7では、マージおよび暗号化により利用条件と復号鍵k d（1）とを不可分に結び付けることを特徴とする。従って、暗号鍵k eによる暗号を復号できる装置、即ち、暗号鍵k eに対応する復号鍵k dを有する装置のみが、利用条件と復号鍵k d（1）とを分離する事ができる。復号鍵k d（1）は、暗号化された課金対象情報を復号するための鍵であるから、結局、課金対象情報と利用条件が不可分に結び付けられることになる。データとして課金対象情報とライセンス情報を分離する事は常に可能である。しかし、適切なライセンス情報なしでは課金対象情報の暗号化を解除してコンテンツを利用する事は出来ないようになっている。

【0066】記録部8は、ライセンス情報を情報蓄積部9に書き込み、次いで、その後ろに暗号化された課金対象情報を書き込むようになっている。

【0067】情報蓄積部9は、例えば、DVD-ROM、DVD-RAM、ハードディスク等の記録媒体であってもよい。このような情報の記録された記録媒体は、所定の再生装置にセッティングされて情報の再生が行われる。あるいは、情報蓄積部9からインターネット等のネットワークを介して転送され、あるいは放送されて、



別の記録媒体に写し替えられ、所定の再生装置で再生されるようになっていてもよい。

【0068】図2は、図1の情報記録装置1の動作を説明するためのフローチャートである。まず、暗号化された課金対象情報〔課金対象情報〕 $k e(1)$ が課金対象情報入力部2に入力され(ステップS1)、利用条件が利用条件入力部4に入力され(ステップS2)、復号鍵 $k d(1)$ が復号鍵入力部5に入力される(ステップS3)。暗号化された課金対象情報は、課金対象情報入力部2から記録部8に転送され(ステップS4)、利用条件は利用条件入力部4から暗号化部7に転送され(ステップS5)、復号鍵 $k d(1)$ は復号鍵入力部5から暗号化部7に転送される(ステップS6)。さらに、鍵保持部6に予め保持されている暗号鍵 $k e$ は、暗号化部7に転送される(ステップS7)。暗号化部7では、利用条件と復号鍵 $k d(1)$ をマージした後、暗号鍵 $k e$ を用いて暗号化してライセンス情報を生成する(ステップS8)。そして、生成されたライセンス情報を記録部8に転送する(ステップS9)。記録部8は、暗号化された課金対象情報とライセンス情報とをマージして情報蓄積部9に記録する(ステップS10)。

#### (1-2) 情報記録装置の第2の例

図3は、本発明に係る情報記録装置の第2の構成例を示したものである。すなわち、図3は、デジタル化された著作物等の課金対象である課金対象情報の一部を利用条件とともに暗号化してライセンス情報を生成し、課金対象情報の残りの部分とライセンス情報を所定の記録媒体に記録する情報記録装置の構成例を示したものである。図1の第1の構成と同様に、課金対象情報と利用条件とを不可分にするために、ここでは、課金対象情報のデータの一部を利用条件と共に暗号化している。

【0069】情報記録装置は、大きく分けてデータ分離部12、ライセンス情報生成部13、記録部18から構成される。

【0070】データ分離部12は、課金対象情報を2つに分割する。データ分離部におけるデータの分離例を図5、図6に示す。説明を簡単にするために、静止画の場合について述べるが、動画その他の場合についても同様な方法を利用することができる。

【0071】図5に示すように、静止画の一部(図5では、顔の領域)を切り取り、図5(b)に示すような顔の領域部分をライセンス情報の一部として暗号化するようにしてもよい。この場合、ライセンス情報を復号しなくても(即ち、利用料金の支払いを行わなくても)画像を見ることはできるが、その画像は一部を欠いていることになる。また、図6に示すように、画像にフーリエ変換を施し、周波数成分を抽出する。そして、図6(b)に示すような高周波成分をライセンス情報の一部として暗号化するようにしてもよい。この場合、ライセンス情報を復号することができなけば(すなわち、利用料金

を払わなければ)、図6(a)に示すような周波数成分の画像を再生しても、不鮮明な映像しか得られない。

【0072】ライセンス情報生成部13は、利用条件入力部14、暗号化部17、鍵保持部16から構成される。

【0073】鍵保持部16には、暗号鍵 $k e$ が予め記憶されている。

【0074】利用条件入力部14には、利用条件が入力する。利用条件とは、課金対象情報の利用期限、ライセンス情報書き込み時刻、コンテンツID、メディアIDあるいは復号ユニットIDのうちの少なくとも1つから構成されている。

【0075】暗号化部17には、利用条件入力部14を介して利用条件が入力し、データ分離部12からは課金対象情報を2分して得られた課金対象情報の一部のデータが入力し、この利用条件と課金対象情報の一部のデータをマージした後、鍵保持部16に記憶されている暗号鍵 $k e$ を用いて暗号化して、ライセンス情報を生成する。

【0076】記録部18は、ライセンス情報を情報蓄積部19に書き込み、次いで、その後ろにデータ分離部12で2分された課金対象情報の残りのデータを書き込むようになっている。

【0077】情報蓄積部19は、例えば、DVD-ROM、DVD-RAM、ハードディスク等の記録媒体であってもよい。このような情報の記録された記録媒体は、所定の再生装置にセッティングされて情報の再生が行われる。あるいは、情報蓄積部19からインターネット等のネットワークを介して転送され、あるいは放送されて、別の記録媒体に写し替えられ、所定の再生装置で再生されるようになっていてもよい。

【0078】図4は、図3の情報記録装置11の動作を説明するためのフローチャートである。まず、課金対象情報がデータ分離部12に入力され(ステップS21)、利用条件が利用条件入力部14に入力される(ステップS22)。データ分離部12は、入力された課金対象情報を2分し(ステップS23)、その結果得られた課金対象情報の一部のデータを暗号化部17に転送し(ステップS24)、課金対象情報の残りのデータを記録部18に転送する(ステップS25)。また、利用条件は利用条件入力部14から暗号化部17に転送され(ステップS26)、暗号鍵 $k e$ は鍵保持部16から暗号化部17に転送される(ステップS27)。暗号化部17では、利用条件とデータ分離部12から転送された課金対象情報の一部のデータをマージした後、暗号鍵 $k e$ を用いて暗号化してライセンス情報を生成する(ステップS28)。そして、生成されたライセンス情報を記録部18に転送する(ステップS29)。記録部18は、データ分離部12から転送された課金対象情報の一部のデータとライセンス情報とをマージして情報蓄積部



19に記録する(ステップ30)。

(1-3) 情報記録装置の第3の例

課金対象情報と利用条件とを不可分にするためのさらに他の例として、課金対象情報の全体を利用条件と共に暗号化することも考えられる。

【0079】図7は、本発明の第1の実施形態に係る情報記録装置の第3の構成例を示したものである。なお、図7において、図3と同一部分には、同一符号を付し、異なる部分について説明する。すなわち、図3のデータ分離部12が図7では、課金対象情報入力部2に置き換わっていて、課金対象情報入力部2に入力された課金対象情報は、そのまま、暗号化部17に転送される。暗号化部17では、課金対象情報の全てと利用条件とをマージした後、暗号鍵k eを用いて暗号化するようになってい

(1-4) まとめ

以上、説明したように、情報記録装置の第1の例では、暗号化された課金対象情報を復号するための復号鍵k d(1)と利用条件とをマージし、暗号鍵k eを用いて暗号化してライセンス情報を生成することにより、利用条件と復号鍵k d(1)とを付加分に結び付けて、暗号化された課金対象情報とライセンス情報とをマージして情報蓄積部9に記録することにより、課金対象情報と利用条件とを不可分に結び付けることができる。この場合、暗号鍵k eに対応する復号鍵k dを有する情報再生装置のみが、利用条件と復号鍵k d(1)とを分離する事ができ、従って、この分離された復号鍵k d(1)を用いて、暗号化された課金対象情報を復号・再生することができる。

【0080】情報記録装置の第2の例では、課金対象情報の一部のデータと利用条件とをマージし、暗号鍵k eを用いて暗号化してライセンス情報を生成し、残りの課金対象情報の一部のデータとライセンス情報とをマージして情報蓄積部19に記録することにより、課金対象情報と利用条件とを不可分に結び付けることができる。この場合、暗号鍵k eに対応する復号鍵k dを有する情報再生装置のみが、課金対象情報の一部のデータと利用条件とを復号・分離する事ができ、従って、この復号・分離された課金対象情報の一部のデータと残りのデータとから課金対象情報を再生することができる。

【0081】情報記録装置の第3の例では、課金対象情報の全データと利用条件とをマージし、暗号鍵k eを用いて暗号化して情報蓄積部19に記録することにより、課金対象情報と利用条件とを不可分に結び付けることができる。この場合、暗号鍵k eに対応する復号鍵k dを有する情報再生装置のみが、課金対象情報のデータと利用条件とを復号・分離・再生することができる。

【0082】これらのいずれも、復号によらずしては、課金対象情報と利用条件とを分離できない様にする為の仕組みを与えるものである。

【0083】また、情報蓄積部9、19は、例えば、DVD-ROM、DVD-RAM、ハードディスク等の記録媒体であってもよい。このような情報の記録された記録媒体は、所定の再生装置にセッティングされて情報の再生が行われる。あるいは、情報蓄積部9、19からインターネット等のネットワークを介して転送され、あるいは放送されて、別の記録媒体に写し替えられ、所定の再生装置で再生されるようになっていてもよい。

(2) 情報再生装置

(2-1) 情報再生装置の第1の例

図8は、本発明に係る情報再生装置の第1の構成例を示したものである。すなわち、図8は、前述の図1の第1の情報記録装置、図3の第2の情報記録装置、図7の第3の情報記録装置で、情報蓄積部9あるいは情報蓄積部19に記録された情報を記録媒体あるいはネットワークあるいは放送にてユーザ分配し、その分配された情報を再生する情報再生装置の構成例を示したものである。

【0084】例えば、第1の情報記録装置で情報蓄積部9に記録された情報の1単位は、暗号化された課金対象情報と、それを復号する復号鍵k d(1)と利用条件とを暗号鍵k eを用いて暗号化して生成されたライセンス情報とをマージしたものである。

【0085】利用条件には、例えば、利用期限が含まれている。利用期限とは、たとえば、ユーザが所定の料金を支払った場合に、その料金に見合った課金対象情報の利用期限である。また利用条件には、ライセンス情報記録時刻が含まれていてもよい。ライセンス情報記録時刻とは、例えば、図1の第1の情報記録装置でライセンス情報が情報蓄積部9に記録された時刻、より具体的には、ライセンス情報生成部3でのライセンス情報生成時に、例えば、利用条件入力部4に具備される時計から読みとられた時刻情報である。

【0086】図8において、情報再生装置は大きく分けて、情報蓄積部101、読み出し部102、復号ユニット103、再生部104から構成される。

【0087】情報蓄積部101は、例えば、DVD-ROM、DVD-RAM、ハードディスク等の記録媒体であってもよい。また、情報蓄積部101に記録されている情報は、図1、図3、図7の情報蓄積部9あるいは情報蓄積部19に記録された情報がインターネット等のネットワークを介して転送され、あるいは放送されて、写し替えられたものであってもよい。

【0088】読み出し部102は、情報蓄積部101から1単位の情報を読み出し、ライセンス情報を復号ユニット103へ転送し、暗号化された課金対象情報を再生部104にそれぞれ転送する。

【0089】復号ユニット103は、予め記憶する復号鍵k dを用いてライセンス情報を復号し、その結果得られた利用条件に基づき、暗号化された課金対象情報を復号する復号鍵k d(1)を再生部104に出力するか否

かを判定することにより、著作権保護を行うようになっている。

【0090】課金対象情報は、暗号鍵 $k_e(1)$ によって暗号化されているため、再生部104に暗号鍵 $k_e(1)$ に対応する復号鍵 $k_d(1)$ が与えられない限り、課金対象情報を再生することはできない。復号鍵 $k_d(1)$ は、復号ユニット103から再生部104に転送されるようになっている。なお、復号鍵 $k_d(1)$ を復号ユニット103から再生部104へ転送する際には、通常保護される。復号鍵 $k_d(1)$ を転送中に取得・保存されると、その後は、復号ユニット103を経由しなくても再生が可能になってしまう。それでは復号ユニット103における利用条件チェック等の著作権保護が無意味になるからである。転送保護の具体的な方法としては、例えば、「日経エレクトロニクス」1996.11.18(No. 676)ニュースレポート(p13-p14)に、その一例を見る事ができる。

【0091】再生部104は、復号部105を具備している。復号部105では、読み出し部102から転送された暗号化された課金対象情報を、復号ユニット103から転送された復号鍵 $k_d(1)$ を用いて復号する。再生部104では、復号部105で復号した結果得られた課金対象情報のデータを表示するための予め定められたデコードを施し、所定の表示装置に表示するようになっている。

【0092】復号ユニット103の構成例を図9に示す。復号ユニット103は、ライセンス情報入力部103a、復号部103b、復号鍵保持部103c、判定部103d、時計参照部103e、時計103fから構成される。

【0093】ライセンス情報入力部103aは、読み出し部102から転送されたライセンス情報を受け取ると、それを復号部103bに出力する。

【0094】復号部103bでは、復号鍵保持部103cに予め記憶されている復号鍵 $k_d$ を用いてライセンス情報を復号し、その結果得られた利用条件、すなわち、利用期限と、復号鍵 $k_d(1)$ を判定部103dに出力する。

【0095】時計参照部103eは、時計103fで示されている時刻(時計時刻)を読みとるようになっている。

【0096】判定部103dは、時計参照部103eから取得した時計時刻(現在時刻を示す)と、利用期限とを比較して、時計時刻 $\leq$ 利用期限である時、課金対象情報の利用可と判断し(すなわち、復号鍵 $k_d(1)$ の出力を可と判定し)復号鍵 $k_d(1)$ を再生部104に出力する。

【0097】利用条件にさらに、ライセンス情報記録時刻が含まれている場合、利用期限のチェックとライセンス情報記録時刻のチェックも行ふ。すなわち、判定部1

03dは、利用期限が有効であるとき、時計時刻とライセンス情報記録時刻を比較し、さらに、時計時刻 $\geq$ ライセンス情報記録時刻が成立する時、復号鍵 $k_d(1)$ を再生部104に出力する。このチェックは「ライセンス情報が記録されたのは過去である」と言う当然の事柄を確認しているだけであるが、重要な意味を持っている。すなわち、時計参照部103eにて参照する時計103fは、常に正確であるとは限らない。特に、時計が極端に遅れることは、利用期限の遵守の観点から、好ましくない。ライセンス情報記録時刻に関する上記のチェックは、時計の遅れに一定の歯止めをかける意味を持っている。例えば、時計が1ヶ月前の時刻を指していたとする。ライセンス情報記録時刻がある日の12:00で、利用期限がその丁度1週間後の12:00であったとする。ライセンス情報記録時刻のチェックを行わない場合、利用者は1週間+1ヶ月の課金対象情報利用が可能になってしまう。ライセンス情報記録時刻のチェックを行う事により、時計が極めて遅れている場合の課金対象情報の利用を禁止する事ができる。

【0098】図10に示すフローチャートは、図8の情報再生装置の処理動作の流れを説明するためのものである。読み出し部102は、情報蓄積部101に記録されている1単位の情報、すなわち、暗号化された課金対象情報とライセンス情報を読み出す(ステップS41)、ライセンス情報を復号ユニット103へ転送し(ステップS42)、暗号化された課金対象情報を再生部104へ転送する(ステップS43)。復号ユニット103では、予め記憶している復号鍵 $k_d$ を用いてライセンス情報を復号し、利用条件(利用期限)と復号鍵 $k_d(1)$ を得る。そして、利用条件(利用期限)に基づき課金対象情報の利用の可否を判断する(ステップS44)。利用期限が有効で課金対象情報の利用が可と判断されたとき(ステップS45)、復号ユニット103は、復号鍵 $k_d(1)$ を再生部104に転送する(ステップS46)。一方、課金対象情報の利用が不可と判断されたときは、復号鍵 $k_d(1)$ の出力不可通知を再生部104に出力し、処理を終了する。再生部104では、復号鍵 $k_d(1)$ を用いて暗号化された課金対象情報を復号し、さらにデコードして課金対象情報を再生する(ステップS47)。

【0099】次に、図11に示すフローチャート、図8、図9を参照して、図10のステップS44～S46の復号ユニット103の処理動作の流れをより詳細に説明する。復号ユニット103のライセンス情報入力部103aは、読み出し部102から転送されてきたライセンス情報を受け取ると(ステップS51)、ライセンス情報を復号部103bに転送する(ステップS52)。復号鍵保持部103cから復号鍵 $k_d$ が転送されると(ステップS53)、復号部103bでは復号鍵 $k_d$ を用いてライセンス情報を復号する(ステップS54)。

ライセンス情報を復号した結果得られたデータは、判定部103dに転送される(ステップS55)。時計参照部103eから時計時刻が転送されてくると(ステップS56)、判定部103dは、利用条件(利用期限)と時計時刻を比較して課金対象情報の利用の可否(すなわち、復号鍵kd(1)を再生部104に出力するか否か)を判定する(ステップS57)。課金対象情報の利用が可と判定されたときは、復号鍵kd(1)を再生部104に出力し(ステップS58~S59)、課金対象情報の利用が不可と判定されたときは、再生部104に復号鍵kd(1)の出力不可通知を出力する(ステップS58、ステップS60)。

(2-2) 復号ユニットの構成および復号ユニットに具備される時計

利用条件として課金対象情報の利用期限を用い、課金対象情報の利用期限限定を行う場合、図9の復号ユニット103に具備される時計103fの正確さは重要である。その意味で、ユーザが任意に時刻設定を行う事を不可能にする仕組みが必要である。図12に、その様な仕組みを有した復号ユニットの構成例を示す。なお、図12において、図9と同一部分には同一符号を付している。

【0100】図12に示すように、時計103fは、時刻設定部111、時刻設定無効化部112、計時カウンタ113から構成される。図13に示すフローチャートを参照して、図12の時計103fの動作を説明する。工場出荷時に設定時刻情報を含む時刻設定指示情報を時刻設定部111を介して入力すると(ステップS71)、時刻設定部111は、その指示された設定時刻を計時カウンタ113に設定する(ステップS72~ステップS73)。その後、時刻設定無効化部112にて、以後の時刻設定部111を介しての時刻設定が無効となるような処置を施す(ステップS74~ステップS75)。時刻設定無効化部112は、例えば、時刻設定部111と計時カウンタ113を結ぶ回路に過電流を流して、時刻設定部111と計時カウンタ113を物理的に遮断するようにしてもよい。時刻設定無効化処置を施された後は、時刻設定は一切不可能になる。

【0101】誤差評価部103gは、最大累積誤差を、例えば、次の様な方法で決定する。誤差評価部は、時計103fの「最大遅れ時」と「最大進み時」を保持している。また、誤差評価用の計時カウンタを具備し、この計時カウンタで毎時最大遅れ、最大進みをそれぞれ加算して、その加算値である累積最大遅れと累積最大進み(これらをまとめて累積誤差と呼ぶ)とを判定部103dに転送する。

【0102】累積最大進み、累積最大遅れとは、例えば、時計103f自体の動作異常により生じる誤差の累積時間である。従って、時計103fにて示される時計時刻と利用期限およびライセンス情報記録時刻とをそれ

ぞれ比較する際には、この累積誤差を加味する必要がある。

【0103】この場合、復号ユニット103の判定部103dは、次式の成立を調べる。

【0104】時計時刻 ≤ 利用期限+累積最大進み  
時計時刻 ≥ ライセンス情報記録(更新)時刻-累積最大遅れ

この2式が同時に成立する時、課金対象情報の利用を可と判定する。第1の情報記録装置により情報蓄積部9に記録された情報を再生する場合には、復号鍵kd

(1)、第2の情報記録装置により情報蓄積部19に記録された情報を再生する場合は、課金対象情報の一部の出力をそれぞれ可と判定する。

【0105】次に、図14に示すフローチャートを参照して、図12の復号ユニットの処理動作について説明する。復号ユニット103のライセンス情報入力部103aは、読み出し部102から転送されてきたライセンス情報を受け取ると(ステップS81)、ライセンス情報を復号部103bに転送する(ステップS82)。復号鍵保持部103cから復号鍵kdが転送されると(ステップS83)、復号部103bでは復号鍵kdを用いてライセンス情報を復号する(ステップS84)。ライセンス情報を復号した結果得られたデータは、判定部103dに転送される(ステップS85)。時計参照部103eが時計103fから時計時刻を取得し(ステップS86)、その取得した時計時刻を判定部103dに転送する(ステップS87)。判定部103dは、さらに、誤差評価部103gから累積誤差を取得すると(ステップS88)、時計103fの累積誤差を加味して、利用条件(利用期限)と時計時刻との比較を行い、課金対象情報の利用の可否(すなわち、復号鍵kd(1)を再生部104に出力するか否か)を判定する(ステップS89)。課金対象情報の利用が可と判定されたときは、復号鍵kd(1)を再生部104に出力し(ステップS90~S91)、課金対象情報の利用が不可と判定されたときは、再生部104に復号鍵kd(1)の出力不可通知を出力する(ステップS90、ステップS92)。

(2-3) 復号ユニットに具備された時計の時刻設定：その1

図15は、復号ユニット103に具備される時計103fの他の構成例を示したもので、暗号化された時刻設定指示情報に基づき時刻設定を行う時計103fの構成例を示したものである。

【0106】図15に示すように、時計103fは、設定時刻入力部121、復号部122、コマンド認証部123、時刻設定部124、計時カウンタ125から構成される。

【0107】このような構成の時計103fの動作について図16に示すフローチャートを参照して説明する。設定時刻情報を含む時刻設定指示情報は予め暗号化さ

れ、その暗号化された時刻設定指示情報が設定時刻入力部121に入力されると(ステップS101)、設定時刻入力部121は、暗号化された時刻設定指示情報を復号部122へ転送する(ステップS102)。復号部122は、暗号化された時刻設定指示情報を復号し(ステップS103)、その復号された時刻設定指示情報をコマンド認証部123へ転送する(ステップS104)。コマンド認証部123は、時刻設定指示情報のコマンド形式を確認し(ステップS105)、正しい形式であるときは(ステップS106)、時刻設定指示情報に含まれる設定時刻情報を時刻設定部124へ転送する(ステップS107)。時刻設定部124は、設定時刻情報に従って計時カウンタ125の時刻設定を行う(ステップS108)。

【0108】時計103fが図15に示した構成であることにより、時計103fに入力される時刻設定指示情報は常に所定の暗号鍵を用いて暗号化されている必要があるため、暗号化を行うことのできない装置(即ち、暗号化用の鍵を保持していない装置)を用いて、時刻設定を行う事は不可能となる。従って、ユーザが安易に時計103fの時刻設定を行うこともできない。

(2-4) 復号ユニットに具備された時計の時刻設定:  
その2

次に、ネットワークを介して復号ユニット103に具備される時計103fの時刻設定を行う場合について説明する。

【0109】図17は、ネットワーク時刻設定の概念図である。時刻設定クライアントは、時刻設定を行うべき時計、すなわち、例えば、図8に示すような第1の情報再生装置の復号ユニット103に具備される時計103fを含んでいる。この時計の時刻をここでは、クライアント時刻と呼ぶことにする。時刻設定サーバも内部に時計を具備し、その時計の示す時刻をここでは、サーバ時刻と呼ぶことにする。このような形態にて、ネットワークを介して時刻設定サーバが時刻設定クライアントの具備する時計の時刻設定を行うわけである。

【0110】復号ユニットに具備された時計の時刻設定の際には、若干込み入った処理が必要である。それは、以下の様な理由による。クライアントの時計201の進み方のチェックを行わなくてはならない。クライアント時刻の1分が、サーバ時刻の1分に、ほぼ等価である事を確認する作業が必要である。この事は、i)サーバが認証情報の送信時刻を指定する事、ii)認証情報到着時刻を指定する事(タイムアウトの設定)により、この確認が行われている。なお、クライアントからサーバに認証情報を送信するのは、虚偽の申告を避ける為である。すなわち、サーバは、認証情報の到着時刻を用いて、クライアント時刻の進み具合を計測しているからである。また、サーバから送信される時刻設定コマンドが、クライアントに到着後、速やかに時計201に入力

される事を保証する必要がある。この事を保証する為に、クライアントの時計201にはタイムアウト(時刻設定指示受信時刻)が設けられている。

【0111】時刻設定クライアントの構成例を図18に示す。図18に示すように、時刻設定クライアントは時計201、ネットワーク通信部202、クライアント認証鍵格納部203、暗号化部204から構成される。

【0112】時刻設定サーバの構成例を図19に示す。

【0113】次に、時刻設定クライアントおよび時刻設定サーバの動作を示す図20～図22のフローチャート、時刻設定クライアントの時計201の構成例を示した図23、およびその動作を示した図24～図25のフローチャートを参照して、ネットワークを介して時刻設定サーバから時刻設定クライアントの時計201の時刻設定を行う動作について説明する。

【0114】先ず、時刻設定クライアントでは、時計201にて示されている現在のクライアント時刻 $t_1$ をネットワーク通信部202を介して、時刻設定サーバに送る(図20のステップS111～ステップS112)。すなわち、図23に示すように、時刻読み出し部302は計時カウンタ301から現在のクライアント時刻 $t_1$ を読み出し(図24のS161)、それを図18のネットワーク通信部202へ出力する(図24のステップS162)。

【0115】時刻設定サーバでは、ネットワーク接続部211を介してクライアント時刻 $t_1$ を受信すると(図21のステップS131)、それを時刻指定部212に転送し(ステップS132)、時刻指定部212は、到着期限時刻設定部213にクライアントからの時刻 $t_1$ の到着を通知するとともに(ステップS133)、 $t_1$ に、予め定められた数値を加えて、認証情報送信時刻(クライアント時刻) $t_2$ を決定し(ステップS134)、それをネットワーク接続部211を介して時刻設定クライアントに転送する(ステップS135)。また、認証情報送信時刻 $t_2$ は指定時刻格納部218に格納される(ステップS136)。到着期限時刻設定部213では、時刻到着通知を受け取ると、時計214から、クライアントからの時刻 $t_1$ の到着時刻(サーバ時刻) $T_1$ を取得し(ステップS137)、 $T_1$ に、予め定められた数値を加えて、認証情報到着時刻(サーバ時刻) $T_2$ を決定し(ステップS138)、それを到着期限時刻格納部215に格納する(ステップS139)。

【0116】時刻設定クライアントでは、ネットワーク通信部202を介して認証情報送信時刻 $t_2$ を受信すると(図20のステップS113)、それを時計201に転送し(ステップS114)、クライアント時刻 $t_2$ まで待つ。クライアント時刻で示される $t_2$ に、時計201は、認証情報を読み出して、時計201は、暗号化部204に出力する。このとき、認証情報は、時刻「 $t_2$ 」であってもよい(ステップS115)。すなわち、

時計201では、図23に示すように、認証情報送信時刻 $t_2$ を受け取ると、指定時刻格納部303にそれを格納する(図24のステップS163)。時刻比較部304では、指定時刻格納部303に格納された認証情報送信時刻 $t_2$ を読み出し、さらに、計時カウンタ301の示すクライアント時刻 $t$ を随時参照して、 $t_2$ と $t$ との比較を行い、これらが一致したとき、時刻読み出し部302へクライアント時刻の読み出しを指示する(図24のステップS164～ステップS168)。この指示を受けて、時刻読み出し部302は、計時カウンタ301の示すクライアント時刻(この場合、時刻 $t_2$ )を読み出し、図18の暗号化部204に出力する(図24のステップS169)。さらに、時刻設定クライアントの時計201は、 $t_2$ に、予め定められた数値を加え、時刻設定指示受信時刻(クライアント時刻) $t_3$ を決定し、それを時刻設定指示受信時刻格納部309に格納する(図24のステップS170)。

【0117】時刻設定クライアントの暗号化部204では、クライアント認証鍵格納部203から暗号鍵 $k's$ が転送されてくると(ステップS116)、認証情報としての時刻「 $t_2$ 」を暗号鍵 $k's$ を用いて暗号化し(ステップS117)、暗号化された認証情報〔 $t_2$ 〕 $k's$ をネットワーク通信部202を介して時刻設定サーバに転送する(ステップS118～ステップS119)。なお、時刻設定サーバでは、暗号鍵 $k's$ に対応する復号鍵 $k'p$ をサーバ認証鍵格納部219に保持しているものとする。

【0118】一方、時刻設定サーバでは、時刻設定クライアントからの暗号化された認証情報をネットワーク接続部211を介して受信すると(ステップS140)、それを到着期限時刻確認部216に転送する(ステップS141)。到着期限時刻確認部216は、先に到着期限時刻格納部215に格納した認証情報到着時刻 $T_2$ を取り出し、暗号化された認証情報を受信した時刻 $T$ (サーバ時刻)を時計214から読み出す(ステップS142～ステップS144)。そして、認証情報の受信時刻 $T$ と認証情報到着時刻 $T_2$ とを比較する。 $T > T_2$ であれば、遅延時間が長すぎると判断し、以後の処理を行わない(ステップS145)。 $T \leq T_2$ ならば、暗号化された認証情報を復号部217に転送し(図22のステップS146)、サーバ認証鍵格納部219に格納されている復号鍵 $k'p$ を用いて復号し(ステップS147～ステップS148)、復号された認証情報を指定時刻確認部220に転送する(ステップS149)。指定時刻確認部220には、さらに、先に指定時刻格納部218に格納された認証情報送信時刻 $t_2$ も転送され、これらを比較することにより、時刻設定クライアントの時計の認証を行う(ステップS150～ステップS152)。ここでは、時刻「 $t_2$ 」を確認する事になる。時刻設定クライアントの時計の認証に失敗すれば、以後の

処理を行わない。時刻設定クライアントの時計の認証に成功すると、指定時刻確認部220は、時刻設定指示生成部221に対し時刻設定指示を送信する(ステップS153)。この指示を受けて、時刻設定指示生成部2212は、時計214からその時点におけるサーバ時刻を読み出し、そのサーバ時刻を含む時刻設定コマンドを生成する。さらに、時刻設定コマンドに、暗号鍵 $k't$ による暗号化を施す。時刻設定クライアントの時計では、暗号鍵 $k't$ に対応する復号鍵 $k'q$ を保持しているものとする(ステップS154～ステップS155)。暗号化された時刻設定コマンドはネットワーク接続部211を介して時刻設定クライアントに送信される(ステップS156～ステップS157)。

【0119】時刻設定クライアントでは、ネットワーク通信部202を介して暗号化された時刻設定コマンドを受信すると、それを時計201に入力する(図20のステップS120～ステップS121)。

【0120】時計201は、図23に示すように、暗号化された時刻設定コマンドを設定時刻入力部305で受け取ると、その旨を時刻設定指示入力時刻参照部310に通知する(図24のステップS171～ステップS172)。この通知を受けて、時刻設定指示入力時刻参照部310は、計時カウンタ301からクライアント時刻 $t$ を取得し、それを時刻比較部311に出力する(図24のステップS173～ステップS174)。時刻比較部311は、時刻設定指示受信時刻格納部309から先に格納された時刻設定指示受信時刻 $t_3$ を読み出し、そのときのクライアント時刻 $t$ と比較する。このとき、時刻比較部311は、許容遅延時間格納部312に予め格納されている許容遅延時間 $\Delta t$ を用いて比較判断を行うようにしてもよい(図24のステップS175～ステップS177)。 $t > t_3 + \Delta t$ であれば、遅延時間が長すぎると判定し、以後の処理を行わない(図24のステップS178)。 $t \leq t_3$ ならば、時刻比較部311は、設定時刻入力部305に対し時刻設定許可を通知する(図24のステップS178～ステップS179)。この通知により、時刻設定クライアントの時計201は、時刻設定サーバから送信された時刻設定指示(コマンド)に基づいて時刻設定動作を行う。

【0121】図23に示すように、時刻設定クライアントの時計201の設定時刻入力部305は、時刻設定許可通知を受け取ると、暗号化された時刻設定指示を復号部306に転送する(図25のステップS180)。復号部306は、暗号化された時刻設定指示を復号鍵 $k'q$ を用いて復号し、復号された時刻設定指示をコマンド認証部307へ転送する(図25のステップS181～ステップS182)。コマンド認証部307は、時刻設定指示のコマンド形式を適否を確認し、正しいコマンド形式の場合は、時刻設定指示中のサーバ時刻を時刻設定部308に転送する(図25のステップS183～ステ

ップS185)。時刻設定部308は、計時カウンタの示すクライアント時刻をコマンド認証部307から受け取ったサーバ時刻に合わせる(図25のステップS186)。

(2-5) 情報再生装置の第2の例：ライセンス情報の更新(利用条件に課金対象情報IDを含む)

課金対象情報には、それぞれを識別するための課金対象情報IDが付されていて、利用条件には少なくとも、利用期限と課金対象情報IDを含むものとする。このような条件のもと、情報再生装置の情報蓄積部に既に格納されているライセンス情報をネットワークを介して更新する場合について説明する。

【0122】図26は、第2の情報再生装置の構成例とライセンス情報を更新するためのシステム全体の構成例を示したもので、第2の情報再生装置は、情報蓄積部401、復号ユニット403、ライセンス情報更新クライアント部403、再生部404、ネットワーク接続部405、電子決済部406から構成される。

【0123】情報再生装置の情報蓄積部401は、図8の第1の情報再生装置の情報蓄積部101と同様である。情報蓄積部401から、図26では省略されている情報読み出し部にて読み出された1単位の情報のうち、ライセンス情報は復号ユニット402に送られる。

【0124】図27は、図26の復号ユニット402の構成例を示したものである。なお、図9と同一部分には同一符号を付し、図9に示した構成とは、利用条件に含まれている課金対象情報IDを出力するための課金対象情報ID出力部103gが追加されている点で異なる。

【0125】次に、図28に示すフローチャートを参照して、図27の復号ユニットの動作について説明する。ライセンス情報は、まず、復号ユニット402のライセンス情報入力部103aに入力し、復号部103bへ送られる(ステップS201～ステップS202)。復号部103bでは、復号鍵保持部103cに保持されている復号鍵kdを用いてライセンス情報を復号し、復号されたライセンス情報を判定部103dに転送する(ステップS203～ステップS205)。時計参照部103eから時計時刻が転送されてくると(ステップS206)、判定部103dは、利用条件(利用期限)と時計時刻を比較して課金対象情報の利用の可否(すなわち、復号鍵kd(1)を再生部404に出力するか否か)を判定する。課金対象情報の利用が可と判定されたときは、復号鍵kd(1)を再生部404に出力する(ステップS206～S209)。ここまでは、図9の復号ユニットの動作と同様である。一方、判定部103dで、課金対象情報の利用が不可と判定されたときは、利用条件に含まれる課金対象情報IDを課金対象情報ID出力部103gに転送するとともに、再生部404へ復号鍵kd(1)の出力不可通知を出力する(ステップS210～ステップS211)。課金対象情報ID出力部10

3gは、課金対象情報IDをライセンス情報更新クライアント部403に出力する(ステップS212)。

【0126】次に、ライセンス情報更新クライアント部403の構成および動作について、主に、図29および図30を参照して説明する。復号ユニット402から送られてくる課金対象情報IDは、ライセンス情報入力部403aに入力される(ステップS221)。このとき、課金対象情報ID以外のライセンス情報をライセンス情報入力部403aに入力するようになっていてもよい。以下、ライセンス情報入力部403aには、少なくとも課金対象情報IDを含むライセンス情報が入力されるものとする。さて、ライセンス情報入力部403aに入力されたライセンス情報は、ライセンス情報転送部403bを経由してネットワーク接続部405に出力され、図26のライセンス情報更新サーバ407に送信されるようになっている(ステップS222～ステップS223)。なお、ライセンス情報転送部403bでは、ライセンス情報を暗号化してからネットワーク接続部405に出力するようにしてもよい。

【0127】その後、図26のライセンス情報更新サーバ407から、課金対象情報IDに対応して、暗号化された支払い要求(フィールドIDを含む)が送信されると、第2の情報再生装置では、暗号化された支払い要求をネットワーク接続部405を介して受信し、ライセンス情報更新クライアント部403の支払い要求入力部403cに転送する(ステップS224)。さらに、暗号化された支払い要求は復号部403dに転送される(ステップS225)。復号部403dでは、暗号化された支払い要求を復号してから、支払い確認部403eへ転送する(ステップS226～ステップS227)。支払い確認部403eは、ユーザに対し、例えば、所定の表示装置に支払い要求の内容を表示して、課金対象情報を利用するための料金支払いの意志を確認する(ステップS228)。ユーザが所定の入力装置を介して料金を支払う旨を指示した場合は、支払い指示部403fに対し、支払い指示の発行を要求する(ステップS229～ステップS230)。支払い指示部403fで生成される支払い指示は、電子決済部406を経由してから所定のネットワークを介して電子決済業者のサーバ408に送信されるようになっている(ステップS231)。

【0128】さて、電子決済業者のサーバ408で、料金の支払いが確認されると、その旨をライセンス情報更新サーバ407に通知するので、その通知を受けて、ライセンス情報更新サーバ407では、例えば、当該課金対象情報の利用期限を延長して新たなライセンス情報を生成し、それを暗号化して第2の情報再生装置へ送信する。第2の情報再生装置では、ネットワーク接続部405で更新されたライセンス情報を受信すると、ライセンス情報更新クライアント部403のライセンス情報入力部403gに入力され、さらに、ライセンス情報更新部

403hに転送される(ステップS232～ステップS233)。ライセンス情報更新部403hは、受け取ったライセンス情報を情報蓄積部401に既に記録されている当該課金対象情報のライセンス情報に上書きすることによりライセンス情報を更新する(ステップS234)。

【0129】次に、ライセンス情報更新サーバ407の構成および動作について、図31および図32を参照して説明する。図30のステップS223で、第2の情報再生装置から送信されるライセンス情報は、ライセンス情報更新サーバ407のネットワーク接続部407aで受信されると、ライセンス情報更新ユニット407bに転送される(図32のステップS241～ステップS242)。ここで、必要があればライセンス情報を復号し、その復号されたライセンス情報は、ライセンス情報データベース407cに登録される(ステップS243)。このとき、ライセンス情報データベース407cでは、ライセンス情報の更新履歴を管理するため、登録の際にライセンス情報にフィールドIDを添付するようになっている。このフィールドIDは、ライセンス情報更新ユニット407bにも通知される。課金データベース(DB)検索部407dは、ライセンス情報に含まれる課金対象情報IDをもとに課金データベース407eを検索し、支払い要求を生成する(ステップS244～ステップS246)。

【0130】支払い要求の内容は、例えば、図33に示すように、課金対象情報ID、その課金対象情報を利用するにあたり支払うべき料金の提示(利用期限と対応する料金)、料金の支払い先等が記述されている。

【0131】生成された支払い要求は、フィールドIDとともに暗号化部407fに転送されて、暗号化された後、ネットワーク接続部407aに転送され、ネットワークを介して第2の情報再生装置に送信されるようになっている(ステップS247～ステップS250)。暗号化された支払い要求とフィールドIDは、第2の情報再生装置で受信され、図30のステップS224以降で説明したような処理される。

【0132】さて、第2の情報再生装置では、図30のステップS231で当該課金対象情報の利用に対する支払いを支払い指示を発行することにより行うが、その際の支払い指示の内容を、ユーザに提示された支払い要求が図33に示したものであるとき、例えば、「10円/1週間 for "ABCD" to abc、整理番号:フィールドID」と記述して、電子決済部406を通じて支払いを行う。ここで、整理番号は、ライセンス情報に付されたフィールドIDである。この支払い指示を受け取った電子決済業者のサーバ408は支払い処理を行った後、「10円/1週間 for "ABCD" from A to abc、整理番号:フィールドID」と言う明細を添えて、ライセンス情報更新サーバ407に支払い確認を送

る。ここで、AはユーザのIDであるとする。

【0133】ネットワーク接続部407gを介して支払い確認を受け取ったライセンス情報更新サーバ407では、まず、ライセンス情報更新ユニット407bにて、整理番号、すなわち、フィールドIDに基づいて、ライセンス情報データベース407cから更新すべきライセンス情報を検索する(ステップS251～ステップS253)。ライセンス情報更新ユニット407bは、さらに、支払い確認を参照して、ライセンス情報中の利用条件を更新し、再び暗号化して(ステップS254)、その暗号化したライセンス情報をネットワーク接続部407aを介して第2の情報再生装置に送信する(ステップS255～ステップS256)。

【0134】ライセンス情報更新サーバから第2の情報再生装置に送信する支払い要求を暗号化するのは、次の理由による。すなわち、支払い要求を送信する通信路はインターネット等の公衆回線であって、一般にセキュリティが保証されていない。従って、例えば、支払い要求が改竄され、ユーザが不正な支払先に支払いを行う危険性が存在する。暗号化によって、それを防止する。

【0135】図34は、図26に示した第2の情報再生装置を含むシステム全体の動作を概略的に説明するためのフローチャートである。なお、図34に示した符号(ステップS261～ステップS286は、図26に示した符号に一致し、その詳細な動作説明は前述した通りであるので省略する。

### (3) ライセンス情報更新ユニット

次に、ライセンス情報更新ユニットについて説明する。ライセンス情報更新ユニットは、ライセンス情報の主に利用条件を更新するためのもので、例えば、前述の第1の情報記録装置により情報蓄積部に課金対象情報とともに記録されたライセンス情報の更新を行い、ライセンス情報更新ユニットを単体で利用することもできる。ライセンス情報を更新するために、ライセンス情報更新ユニットは、ライセンス情報に施されている暗号化を解除(復号)し、そこに別途入力された希望利用条件を入力し、その利用条件に対する支払いが行なわれたかを確認した後、それを暗号化し、更新されたライセンス情報として出力する必要がある。

【0136】図35にライセンス情報更新ユニットの構成例を示し、以下、図36～図37に示すフローチャートを参照して、図35のライセンス情報更新ユニットの構成および動作を説明する。

【0137】ライセンス情報更新処理に当たっては、まず、ライセンス情報入力部501へライセンス情報、希望利用条件入力部506へ希望利用条件が入力される(図36のステップS301、図37のステップS308)。ここでいうライセンス情報は、第1の情報記録装置で説明した利用条件と暗号化された課金対象情報の復号鍵kd(1)から構成されている。また、希望利用条

件はユーザが希望する利用条件のことで、ユーザ側から適切なインターフェースを通して入力されるものとする。

【0138】ライセンス情報入力部501に入力したライセンス情報は、復号鍵保持部503に保持されている復号鍵を用いてライセンス情報復号部502で復号され（図36のステップS302）、利用条件と課金情報復号鍵を分離し、ライセンス情報（特に利用条件）を更新可能な状態にするとともに、課金対象情報ID等の課金に必要な情報を支払要求出力部507に送る（図36のステップS303、図37のステップS310）。更に更新可能な状態になったライセンス情報をライセンス情報更新部505で希望利用条件入力部506で入力された利用条件に書き換える（図36のステップS304）。一方、希望利用条件に対する課金を行なうため、希望利用条件入力部506では入力された希望利用条件に対する課金を促すため、支払要求出力部507に希望利用条件の出力を行なう。支払要求出力部507では、希望利用条件入力部506から入力された希望利用条件とライセンス情報復号部502から入力された課金対象情報ID等の課金に必要な情報を予め定められた一定のプロトコルで装置外部に出力する（図37のステップS310）。この出力に基づき外部装置では課金の具体的な手続きに入る。また、ここで出力される支払い要求情報はライセンス情報更新ユニットが組み込まれる著作権保護・課金のための情報流通システム（すなわち、本発明の情報記録装置、情報再生装置から構成される情報流通システム）の利用環境によって決まり、課金対象情報の著作権者が特定されている状況では課金対象情報IDの出力は不要になるし、また、全課金対象情報について利用条件が予め定められている場合には希望利用条件入力部506の存在や支払い要求出力部507からの利用条件の出力も不要になる。このように本実施形態のライセンス情報更新ユニットはそれが利用される環境により、いくつかの自明なバリエーションがあり得る。

【0139】次に、支払要求情報に対する料金の支払いが完了した段階で、外部装置から支払い確認部508に支払い確認の信号が送られ、この信号が送られた時点で、ライセンス情報更新部505から入力された更新ライセンス情報を更新ライセンス情報暗号化部509に送り、暗号鍵保持部510に保持されている予め定められた暗号化鍵で暗号化する（図36のステップS305、ステップS306）。この時、前記信号がくるまで更新されたライセンス情報は更新ライセンス情報暗号化部509へは送られない。この機能により本実施形態のライセンス情報更新ユニットは支払いが行なわれないにも関わらず更新ライセンス情報が出力されるのを防いでいる。

【0140】更新ライセンス情報暗号化部509で暗号化された更新ライセンス情報は、更新ライセンス情報出

力部511に送られ、外部装置に出力される（ステップS307）。ここで課金対象情報IDとは、課金対象情報のIDであって当該情報の著作権者を示し、課金額もしくは被課金者を特定するのに必要な情報である。

【0141】なお、図35に示したライセンス情報更新ユニットは、前述の第1の情報記録装置にて記録媒体等に記録されたライセンス情報の更新みならず、その変形例である第2、第3の情報記録装置にて記録媒体等に記録されたライセンス情報を更新する際にも適用できる。

【0142】さらに、図35に示したライセンス情報更新ユニットは、単体として用いることも、本発明の情報再生装置と組み合わせて、あるいは情報再生装置内に内蔵して用いることもできる。また、図31のライセンス情報更新サーバのライセンス情報更新ユニット407bとして用いることもできる。

#### （4）著作権保護のための課金装置

図38は、前述の情報記録装置にて記録媒体等に記録されたライセンス情報に基づき著作権保護のための課金を行う課金装置の要部の構成例を示したものである。

【0143】図38において、まず、磁気ディスクやDVDディスク及びコンパクトディスクなどの記録媒体615からライセンス情報読み込み部601でライセンス情報を読み込み、それと同時にキーボードやマウスなどの入力媒体616を介して希望利用条件入力部602から希望利用条件を入力する。ライセンス情報及び希望利用条件はライセンス情報更新ユニット603に入力され、前述のライセンス情報更新ユニットの場合と同様なライセンス情報更新処理を経て、支払要求としての課金情報を課金情報検索部604に送る。ここで課金情報とは希望利用条件及び被課金者を特定するのに必要な情報である。課金情報検索部604では、これらの課金情報を基に課金情報データベース609を用いて課金額情報を検索する。また、課金額が予め定まっているような場合は、ライセンス情報更新ユニット603から敢えて希望利用条件を出力することをせず、課金額そのものを出力することもできる。この場合課金情報検索の必要はなくなる。更に課金対象情報の著作権者が特定されている場合はライセンス情報更新ユニット603から課金対象情報ID等の課金情報を出力する必要もなくなる。この場合後に述べる課金履歴管理部608では課金額情報のみを管理すればよく、課金対象情報IDを管理する必要はなくなる。このようにライセンス情報更新ユニット603から出力される課金情報は本課金装置が応用される状況により、自明な変形がありうる。

【0144】次に、課金情報および課金額情報は課金額情報出力部605に送られ、ユーザに課金額が提示される。ユーザが提示された課金額を何らかの方法で支払うと、続く支払い判定部606で支払いの確認が行なわれ、支払いが行なわれた旨の信号が前述のライセンス情報更新ユニットの支払い確認部508に送られる。ここ



で述べているユーザの課金額支払いの方法は現金支払いによる場合は紙幣・硬貨挿入部とそれらの判定部を有し、この判定部の判定に応じて支払い判定部606に信号を送る。また、支払いは電子マネーである場合やクレジットカードもしくはプリペイドカードである場合など様々であり、各々に独自の判定の仕方が存在する。

【0145】支払い判定部606で支払い完了の判定がでたら、支払い判定部606は課金履歴管理部608に課金情報を送りそれらを保存管理する。

【0146】本実施形態の課金装置は、外部とネットワーク等で接続されていないことを前提としているので課金決済はその場では完了しない。故に本実施形態はこのような支払いをどのように分配するかを管理する必要がある。課金履歴管理部608が必要となる。ここに蓄積された履歴情報は定期的に一定の管理者によって読み取られ、しかるべき手段で決済される。

【0147】最後に、支払い判定部606からの支払済みの信号を受けたライセンス情報更新ユニット603は、前述のライセンス情報更新ユニットと同様な手続きを経て更新ライセンス情報を更新ライセンス情報書き込み部607に出力し、書き込み部607は更新ライセンス情報を入力記録媒体615の適切な箇所に書き込む。本実施形態の課金装置を本発明の情報再生装置と組み合わせれば、いわばライセンス情報の更新機能を持った著作権のある情報の自動販売機のようなものを構成できる。すなわち、本発明の特徴的な機能が1つの匡体の中で実現されるところに特徴がある。このように構成することにより、著作権のある課金対象情報をレンタルもしくは販売する場合、持ち運び可能なDVDやCDその他の記録媒体に（暗号化された）課金対象情報が既に入力されているという仮定のもとで、その記録媒体を本実施形態の課金装置に入力することで適切な課金処理を行なうことができ、いつでも誰でも手軽にコンテンツの利用権を買うことができる。

（4-1）課金対象情報の不正コピーの防止対策を講じたライセンス情報更新ユニットおよびそれに対応する情報再生装置の復号ユニット

容易に分かるように、コピーライトのある課金対象情報に永久利用を認めたり、非常に長い利用期限を認めたりすると、その記憶媒体そのものが複製される危険があり、もし複製品が大量に出回ったら、コピーライトは保護できなくなる。このことを解決するために、本実施形態の復号ユニットおよびライセンス情報更新ユニットは、利用条件として永久利用あるいは非常に長い利用期限を許可する場合、手持ちのただ1つの復号ユニットのみに課金対象情報の再生を限定しようとするものである。なお、以下の説明において、利用条件として「無期限」あるいは「永久利用」とあるのは、永久利用あるいは非常に長い利用期限を許可する場合を含むものとする（後述（4-2）の説明およびその他の説明においても

同じ）。このようにすれば違う復号ユニットを使って利用しようとしても利用拒否することができ、例えば複製してもあまり利益がなくなるので、逆にコピーライトが保護される。しかし、この場合、課金対象情報永久利用権購入時に復号ユニットID（復号ユニットを特定するID）が分からないと購入できないことになってしまう。このため、本実施形態のライセンス情報更新ユニットは永久利用権購入コンテンツを最初に利用する時に利用条件に復号ユニットIDを付加することを特徴としている。なお、復号ユニットIDは、各復号ユニットのそれぞれを識別するための識別情報であり、例えば、各復号ユニットの製造番号であってもよい。

【0148】図39は、本実施形態の復号ユニットの構成例を示したものである。以下、図40に示すフローチャートを参照して復号ユニット701の構成および動作について説明する。

【0149】ライセンス情報がライセンス情報入力部711から入力されると（ステップS401）、それが復号部712へ送られ、復号部712では、復号鍵保持部713に保持された復号鍵でライセンス情報を復号する（ステップS402）。復号されたライセンス情報は利用条件変更必要性判定部714に送られる（ステップS403）。利用条件変更必要性判定部714では、利用条件中の利用期限が無制限である場合、それが特定の復号ユニットIDに限定されているか否かを判定し、限定されない場合、利用条件変更の必要ありと認め、その更新をライセンス情報更新ユニット702に委ねるようになっている。すなわち、利用条件変更必要性判定部714では送られた復号されたライセンス情報から利用条件を読み込み利用期間が無制限か否かの判定を行なう（ステップS404）。無制限であつたら利用条件が復号ユニットIDに限定されているか否かを判定し（ステップS405）、限定されていれば、判定部715に利用条件を送り、判定部715では復号ユニットID参照部716に復号ユニットIDの提示の指示を送り（ステップS406）、同参照部716から提示された復号ユニットIDと利用条件に記載されていた復号ユニットIDを比較し（ステップS407）、一致した場合、暗号化された課金対象情報（コンテンツ）の復号鍵kd

（1）を出力して終了し（ステップS408）、一致しない場合たとえばNULLコード（通常は0）を出力して復号出来ない旨の指示とし、終了する（ステップS409）。また、利用条件が無期限で復号ユニットIDが記載されていない場合、利用条件変更必要性判定部714は利用条件に復号ユニットIDを記載する必要を認め、復号ユニットID参照部716から復号ユニットIDを取得し、その取得した復号ユニットIDと暗号化されたライセンス情報とをライセンス情報更新ユニット702に送る（ステップS410）。

【0150】さらに、利用条件が無期限でない場合は

(ステップS404)、利用条件を判定部715に送り、判定部715では時計参照部717から現在時刻の提示を受け(ステップS411)、その時刻から利用の可否を判定し、可の場合は暗号化された課金対象情報(コンテンツ)の復号鍵kd(1)を出力し終了し(ステップS412～ステップS413)、否の場合は前述同様NULLコードを出力し終了する(ステップS414)。

【0151】図41は、ライセンス情報更新ユニット702の構成例を示したものである。以下、図42に示すフローチャートを参照しながら、図41のライセンス情報更新ユニット702の構成および動作について説明する。

【0152】ライセンス情報更新ユニット702は、ライセンス情報入力部721に入力されたライセンス情報をライセンス情報復号部723に送り、ライセンス情報復号部723でその情報を復号鍵保持部724からの復号鍵を基に復号する(ステップS421～ステップS422)。復号されたライセンス情報はライセンス情報更新部725に送られ、そこから利用条件が抽出される(ステップS423)。一方、復号ユニットID入力部722に入力した復号ユニットIDは、ライセンス情報更新部725に送られ(ステップS424)、ライセンス情報更新部725では、先に抽出された利用条件に復号ユニットIDの限定を付加し、利用条件を更新する(ステップS425)。さらに、この更新された利用条件を基に新たなライセンス情報を生成し、それを更新ライセンス情報暗号化部726に送る。更新ライセンス情報暗号化部726では、暗号鍵保持部727から提示された暗号鍵を基に更新されたライセンス情報を暗号化した後(ステップS426)、更新ライセンス情報出力部728に送り、ライセンス情報更新ユニット外部702外部に送り出す(ステップS427)。

【0153】なお、ライセンス情報更新ユニット702と復号ユニット701とを一体化させ、1つのユニットとし、例えば、図38の情報流通システムのライセンス情報更新ユニット603に置き換えることも可能である。

(4-2) 課金対象情報の不正コピーの防止対策を講じた復号ユニットの他の例

前述の(4-1)で述べたように、永久利用権あるいは非常に長い利用期限が認められている(以下、この2つの場合を永久利用権の範疇に含めるものとする)課金対象情報は複製されることによってコピーライトが保護できない状態になる可能性がある。この問題は前述の(4-1)で述べたライセンス情報更新ユニットおよびそれに対応した復号ユニットを用いることにより、ほぼ解決している。即ち、永久利用権の認められている課金対象情報の利用を1つの復号ユニットIDに限定しようとするものであった。この場合問題になるのは永久利用権購

入時に購入者が持つ復号ユニットIDが分らないことがあり得るという点であった。そこで、次に示す第2の復号ユニットでは、永久利用権を取得した課金対象情報を最初に利用する場合、永久利用の旨を記載するところに利用する復号ユニットIDを書き込み、以後その復号ユニットIDでしか復号できないようにした。

【0154】しかしながら、この方式の場合、最初に利用する前に複製される危険があり、ここで複製された永久利用権のある課金対象情報が大量に流布すればやはりコピーライトは保護できなくなる。そこで、第2の復号ユニットでは、永久利用の利用条件にメディアIDを含め、利用時にこれを参照することの特徴としている。ここでメディアIDとは、DVDやCDディスクであればその製造番号であり、一般に、後から改変出来ないROM領域に書かれていることを前提としている。この利用条件が特定のメディアIDに限定されていることから他のメディアに複製されても複製側のメディアIDがオリジナルのメディアIDと異なるため利用条件に合わず利用できないことになる。

【0155】図43は、第2の復号ユニットの構成例を示したものである。以下、図44に示すフローチャートを参照して図43の第2の復号ユニットの構成および動作について説明する。

【0156】ライセンス情報は、ライセンス情報入力部741に入力され、復号部742に送られる(ステップS431)。復号部742では、復号鍵保持部743に保持されている復号鍵を用いてライセンス情報の復号を行ない、利用条件とその他のものとを分離する(ステップS432)。分離された利用条件は利用条件変更必要性判定部744に送られ、ここで利用条件に復号ユニットIDの限定を入れるか否かを判定する。すなわち、前述の(4-1)でも詳しく述べたように利用期限が無期限で、かつ、復号ユニットIDが特定の復号ユニットに限定されていない利用条件には復号ユニットIDの限定を入れなければならない、この場合のみ利用条件変更の必要があると解釈され、復号ユニットID参照部746から復号ユニットIDを取得し、抽出されたライセンス情報と共にライセンス情報更新ユニット732に送る(ステップS434、ステップS435、ステップS447)。その他の場合は利用条件情報を判定部745に送り、利用条件の判定を行なう。

【0157】判定部745では次のような処理を行ない、利用条件が有効なものか否かを判定する。まず、利用条件が無期限であって、復号ユニットIDに限定されている場合、利用条件にメディアIDの限定があるか否かを判定し、ある場合にはメディアID保持部748に保持された当該課金対象情報が入っているメディアのメディアIDを参照し、それと利用条件の限定となっているメディアIDとの比較を行ない、一致していれば復号鍵kd(1)を出力し終了する(ステップS434～

テップS440)。一致していなければ利用拒否の旨の信号、この場合はNUL Lを出力し処理を終了する(ステップS441)。メディアIDの限定がない場合には(ステップS438)、復号鍵k d(1)を出力し終了する(ステップS442)。なお、ここで参照されるメディアIDはメディアID入力部747からのメディアIDの入力を受けメディアID保持部748に保持されている。

【0158】一方、利用条件が有期限の場合(ステップS434)、まず、時計参照部749を介して現在の時刻を参照し(ステップS444)、その時刻が期限内かどうかを判定する(ステップS445)。期限内でない場合、利用拒否の旨の信号、この場合はNUL Lを出力し終了する(ステップS446)。期限内である場合は、ステップS438に進み、利用条件にメディアIDの限定があるか否かを判定し、以降、無期限の場合と同様のアルゴリズムで利用条件の有効性を判定し、その結果によってそれぞれ出力し終了する。

【0159】なお、メディアIDの趣旨から有期限の場合の利用条件にはメディアIDの限定は必要ないように思われるかもしれないが、有期限といっても期間が長い場合もあり、このような場合はその期間内はコピーライトを十分には保護できない。更に例えば期間内であっても無闇に複製されては不都合となる課金対象情報もあり、この場合にも第2の復号ユニットは有効である。

【0160】同様のことは、復号ユニットIDに関しても言えるので、有期限の利用条件であっても利用条件の復号ユニットIDの限定は有効であり、その実現は前述のメディアIDの限定の場合と同様である。また、このことは、前述の(4-1)についても同様である。

#### (5) コピー装置

図45に、例えば、図1の第1の情報記録装置にて記録媒体等に記録された情報のコピーを行うコピー装置の構成例を示す。以下、図46に示すフローチャートを参照して図45のコピー装置の構成および動作について説明する。

【0161】コピーの基本的な考え方は、情報コピーの際の利用条件のデフォルト化である。すなわち、あるメディア(図45のメディア801)に記録されている課金対象情報のライセンス情報は、有効な利用条件を含んでいるかも知れないが、図45のコピー装置では、その複製を作成する際に、この利用条件を消去して、他のメディア(図45のメディア802)に記録するようになっている。

【0162】まず、コピー元のメディア801に記録されている1単位の情報(例えば、暗号化された課金対象情報とそのライセンス情報)を読み出し部803で読み出し(ステップS501)、ライセンス情報のみをライセンス情報複製ユニット804へ転送する(ステップS502)。一方、読み出し部807は、コピー先のメデ

ィア802のメディアIDを読みとり、それをライセンス情報複製ユニット804に転送する(ステップS503～ステップS604)。ライセンス情報複製ユニット804は、コピー元のメディア801から読み出されたライセンス情報をデフォルト化し、コピー先のメディア802のメディアIDを利用条件に書き込むことにより、ライセンス情報を更新し(ステップS505)、その更新されたライセンス情報を書き込む部806に出力する(ステップS506)。

【0163】ライセンス情報複製ユニット804は、例えば、図47に示すような構成である。以下、図48に示すフローチャートを参照してライセンス情報複製ユニット804の構成および動作についても説明する。

【0164】ライセンス情報がライセンス情報複製ユニット804のライセンス情報入力部811に入力すると(図48のステップS511)、復号部812に転送され(ステップS512)、ここで復号される(ステップS513)。復号されたライセンス情報はライセンス情報更新部813に転送される(ステップS514)。一方、コピー先のメディア802のメディアIDはメディアID入力部814に入力され(ステップS515)、ライセンス情報更新部813に転送される(ステップS516)。ライセンス情報更新部813は、コピー元のメディア801から読み出されたライセンス情報の利用条件をデフォルト化し、さらに、コピー先のメディア802のメディアIDを利用条件に書き込み、ライセンス情報を更新する(ステップS517～ステップS518)。この更新されたライセンス情報はライセンス情報出力部815に転送されて(ステップS519)、図45の書き込み部806に出力される(ステップS520)。

【0165】図45の説明に戻り、書き込み部806は、更新されたライセンス情報をコピー先のメディア802に書き込むとともに、読み出し部803から転送されてきた課金対象情報を同じくメディア802に書き込み、コピー処理を終了する(図46のステップS507～ステップS509)。

【0166】このように、図45のコピー装置では、ライセンス情報複製ユニット804でコピー元のメディア801から読みとったライセンス情報の利用条件を消去するため、コピー先のメディア802に記録されている課金対象情報は、メディア801のそれと同一でありながら、ライセンス情報に有効な利用条件を含まないようになっている。従って、メディア802に記録されている情報を、例えば、図43に示したような復号ユニットを具備する情報再生装置で再生しようとしても、その利用が拒絶される。すなわち、ライセンス情報の復号が可能であるのは復号鍵を有する復号ユニットのみであり、課金対象情報の暗号化を解除する為にはライセンス情報に含まれる課金対象情報用の復号鍵が必要であるから、

結局、当該課金対象情報は、そのままでは、利用不可能である。メディア802に複製された課金対象情報を利用する為には、何らかの正当な課金手続きを経て、有効な利用条件をライセンス情報に添付しなければならないことになる。

【0167】なお、利用条件のデフォルト化は、有効な利用条件の消去に限るものではない。例えば、コピー後一日だけ有効とする利用条件を記入する事も可能である。すなわち、例えば、現在が4月16日の13:00であるとすれば、4月17日の23:59を利用期限とする利用条件を記入する。

【0168】さらに、図45のコピー装置は、利用条件をデフォルト化するとともに、コピー先のメディア802のメディアIDの書き込みを行うが、メディアIDは、課金対象情報が記録されているメディアを特定する文字列であり、例えば、DVD-RAMのROM領域に記入されている製造番号である。あるいは、ハードディスク装置の製造番号であってもよい。

【0169】本実施形態では、メディアIDはライセンス情報に含まれている。メディアIDを利用する復号ユニットは、ライセンス情報復号時にメディアIDの確認を行い、再生しようとしている情報の記録されているDVD-RAMのメディアIDが、ライセンス情報に含まれているメディアIDに一致しない場合、前述したように、課金対象情報復号用の復号鍵を出力しないようになっている。復号ユニットが、この様な動作を行う事は、課金対象情報自身が、その「入れ物」を指定する効果を生じさせる。

【0170】ライセンス情報がメディアIDを含む課金対象情報は、本実施形態に述べる様な、正統な(i.e. 復号鍵を有する)コピー装置によってのみ、コピー可能である。コピー先のメディア802をメディアIDの確認を行う復号ユニットを備えた情報再生装置によって再生可能とする為には、メディア802のメディアIDをライセンス情報の利用条件中に埋め込む必要がある。図45のコピー装置は、この処理を行っている。

(6) 情報再生装置の第3の例：副情報(広告や著作権の利用に関する警告等)の視聴に復号ユニットを利用する情報再生装置

図49は、第3の情報再生装置の構成例を示したものである。本発明の情報記録装置により記録媒体等に記録された情報に含まれる副情報(広告や著作権の利用に関する警告等)の視聴の確実を期するため、副情報の中に視聴確認データがちりばめられている。例えば、副情報中の少なくとも2カ所以上に視聴確認データがちりばめられている。副情報の一例を以下に示す。

【0171】「始0Th0めに、ロゴスはおられた。0is0ロゴスは神とともにおられ00た。ロ0is0ゴスは0th0神であった。この方は始めに神と0e c 0ともにおられた。一切のもの0ert i0はこの方

よってできた0fi0。できたもので0cat0この方によら0ion0ずにでき0da0たものは、ただの一つも0ta. 0な00い。」図49の視聴確認データ抽出部903では、入力された副情報を再生部905に送り再生すると同時に、その副情報を順に調べ、2つの「0」で囲まれた文字を取り出していく。2つの「0」の間が空であれば、取り出した文字列を格納する。上記の例では、「this is the certification data.」という文字列が視聴確認データとして抽出され、視聴確認データ抽出部903に具備される所定のメモリに格納されることになる。このように、副情報中の少なくとも2カ所以上に視聴確認情報をちりばめることがポイントである。副情報中に視聴確認情報をちりばめることにより、副情報を全て再生しない限り、視聴確認データを再生することができない。従って、視聴確認データをもって、視聴の確認と見なすことができる。

【0172】以下、図50に示すフローチャートを参照して、図49の第3の情報再生装置の構成および動作について説明する。

【0173】情報蓄積部901は、図8の第1の情報再生装置の情報蓄積部101と同様である。情報蓄積部901から、情報読み出し部902にて読み出された1単位の情報には、暗号化された課金対象情報とそのライセンス情報と副情報が含まれている。そのうち、暗号化された課金対象情報を再生部905に転送し(ステップS601)、副情報を視聴確認データ抽出部903へ転送する(ステップS602)。視聴確認データ抽出部903では、副情報を走査して視聴確認データを抽出する(ステップS603)。読み出し部902は、ライセンス情報を復号ユニット904へ転送する(ステップS604)。

【0174】ライセンス情報の利用条件中には、当該課金対象情報の再生条件として視聴確認データが含まれている。復号ユニット904は、視聴確認データ抽出部903が確認している視聴確認データを読み出し、照合を行う(ステップS605～ステップS606)。視聴確認データが求めるものに一致していれば、続く処理を行う(ステップS607)。すなわち、利用期限等他の利用条件の確認を行った後、課金対象情報の復号用の鍵を再生部905に出力し、課金対象情報の再生を行う(ステップS608～ステップS611)。

【0175】図51は、復号ユニット904の構成例を示したものである。以下、図52に示すフローチャートを参照して復号ユニット904の構成および動作について説明する。

【0176】復号ユニット904に転送されたライセンス情報は、ライセンス情報入力部904aに入力し(ステップS621)、復号部904bに転送される(ステップS622)。復号部904bでは、復号鍵保持部9

04cに保持されている復号鍵kdを用いてライセンス情報を復号した後、視聴確認部904dに転送する(ステップS623～ステップS625)。一方、視聴確認データ抽出部903から送られてきた視聴確認データは、視聴確認データ入力部904eに入力され、視聴確認部904dに転送される(ステップS626)。視聴確認部904dでは、ライセンス情報の利用条件中に含まれる当該課金対象情報の再生条件としての視聴確認データと、視聴確認データ抽出部903から送られてきた視聴確認データとを照合し(ステップS627)、これらが一致しているとき、ライセンス情報を判定部904fに転送する(ステップS628～ステップS629)。判定部904fでは、ライセンス情報中の利用条件に基づき課金対象情報の利用の可否(すなわち、復号鍵kd(1)を再生部905に出力するか否か)を判定して、その判定結果に応じて、復号鍵を再生部905に出力する(ステップS630～ステップS632)。

(追記)以上説明した本発明の情報記録装置では、1つの課金対象情報に対し1つのライセンス情報を対応させて記録媒体等に記録する場合に限らず、1つの課金対象情報に対し、複数のライセンス情報を対応させて記録媒体等に記録するようにしてもよい。

【0177】また、本発明の情報再生装置では、課金対象情報の利用の可否を判定する場合、該課金対象情報に対応する1つのライセンス情報に含まれる利用条件を参照するようになっているが、この場合に限らず、記録媒体に1つの課金対象情報に対応して複数のライセンス情報が記録されている場合には、これら全てのライセンス情報に含まれる利用条件を順次参照して該課金対象情報の利用の可否を判断するようにしてもよい。すなわち、複数のライセンス情報のそれぞれに含まれる利用条件のうち、条件を満たすものが1つでもあれば、該課金対象情報の利用を可能と判断する。

【0178】また、本発明の情報再生装置および課金装置において、ライセンス情報を更新する際には、既に記録媒体に記録されているライセンス情報を書き換える場合に限らず、該記録媒体に追加記録することも可能である。従って、上記実施形態の記録媒体等に記録されたライセンス情報の更新に関する説明中、「更新」は、「上書き記録」と「追加記録」を含むものである。

【0179】さらに、利用条件に含まれる復号ユニットID、メディアID等は、必ずしも1つである必要はない。

(第2の実施形態)

(1) 復号ユニットA

図54は、第2の実施形態に係る復号判定装置、すなわち、復号ユニットAの構成例を示したものである。

【0180】復号ユニットAは、主にデジタルコンテンツである有料データに付属するライセンス情報を基に当該コンテンツの利用が可能か否か(すなわち、例えば契

約により定められた利用条件に基づく該コンテンツ情報の利用のライセンスが有効か無効か)のチェックを行い、有効ならば該コンテンツ情報を利用するためのコンテンツ復号鍵をビデオ再生装置などのコンテンツ情報の再生等を行うための情報利用装置に出力するものである。

【0181】尚、ここではコンテンツ情報は予め暗号化されていて、その復号鍵(以下コンテンツ復号鍵という)を利用有効期限等のコンテンツ利用条件や当該コンテンツ情報の識別情報(ID)などとともにライセンス情報に入れ、当該ライセンス情報全体を暗号化して、暗号化されたコンテンツ情報とともに契約ユーザに提供する(例えば、放送配信、記録媒体に格納して配布等)。

【0182】ライセンス情報の復号は復号ユニットA内に存在する秘密鍵で行う。図55にライセンス情報の一例を示す。図55に示すように、ライセンス情報には、少なくともコンテンツ復号鍵、当該コンテンツ情報の利用有効期限等のコンテンツ利用条件、当該コンテンツ情報のIDが含まれている。

【0183】ライセンス情報を復号する秘密鍵が全ての復号ユニットに共通のものであると、運用上は便利ではあるが、ひとたびこの秘密鍵が外部に洩れればこの復号ユニットを使って復号されるライセンス情報に含まれるコンテンツ復号鍵が原理的に全て読み取れることになる。これはライセンスを保護することを目的とする復号ユニットAとしては深刻な問題であり、これを解決するのが本発明の目的である。

【0184】本実施形態の復号ユニットAでは、この問題点を解決するため、ライセンス情報を復号するための秘密鍵を復号ユニットA内で生成し、これをある一定期間に限って用いるようになっている。

【0185】次に、図57に示すフローチャートを参照して、図54の復号ユニットAの各構成部の動作について説明する。

【0186】暗号化されたライセンス情報は、ライセンス情報入力部2001を通じて復号ユニットA内に入力され(ステップS1001)、復号部2002で復号された後(ステップS1002)、判定部2003に送られ、利用条件のチェックにより当該ライセンスが有効か否かが判定される(ステップS1003～ステップS1004)。ここで、ライセンスが有効か否かの判定とは、利用条件が満たされているか否か、すなわち、例えば、当該コンテンツの利用有効期限を経過していないか否かを判定するものとする。

【0187】判定部2003にて有効(コンテンツの利用可能)という判定が出ればライセンス情報に含まれるコンテンツ復号鍵を情報利用装置2020に出力する(ステップS1005)。

【0188】一方、無効(コンテンツの利用不可)という判定が出れば当該ライセンス情報を更新情報生成部2

004に送り、ライセンスの更新(すなわち、ライセンス情報の更新)に必要な情報をまとめ、ライセンス情報を更新するための更新情報を生成して、ライセンス情報更新装置2008に例えば所定の通信回線(例えば、専用回線、インターネット等でもよい)を経由して出力する(ステップS1006〜ステップS1010)。

【0189】更新情報生成部2004は、利用条件入力部2009を介して入力されたユーザの希望する利用条件(利用期限の延長等)と、判定部2003から送られたライセンス情報とに基づき、少なくとも当該コンテンツのID、鍵生成部2006で生成された復号ユニットAの公開鍵を含む更新情報(図56参照)を生成するようになっている。

【0190】復号ユニットAには、前述したように、暗号化されたライセンス情報を復号するための秘密鍵を生成する鍵生成部2006を具備している。鍵生成部2006では、ライセンス情報を暗号化/復号化するための鍵を生成する。鍵生成手法としては、例えば、公開鍵暗号の鍵生成のアルゴリズムを用いてもよく、RSA暗号の場合は乱数と素数判定アルゴリズムを用いて適当な長さ(例えば、512bit程度)の2つの素数 $p$ 、 $q$ を生成する。

【0191】ここで乱数のアルゴリズムは全ての復号ユニットAで共通であっても、乱数の種の取り方に時間のマイクロ秒をとるなどの工夫をすれば同じ素数が生成される可能性は極めて低い。

【0192】次に、 $N=p \cdot q$ とし $N$ を求める。同時に、 $M=(p-1)(q-1)$ を求め、

【0193】

【数1】

$$e \cdot d \equiv 1 \pmod{M}$$

となるような整数 $e$ 、 $d$ ( $0 < e, d < M$ )を求める。 $e$ 、 $d$ は、まず、 $d$ を決め、それに対応する $e$ をユークリッドの互除法というアルゴリズムを用いて求めるようにすると比較的容易に求められる。この一方(例えば $e$ )を秘密鍵、他方(例えば $d$ )と $N$ を公開鍵とすれば、これらの鍵を使い、公知のRSA暗号のアルゴリズムによって公開鍵暗号が実現される。

【0194】さらに、これらの鍵は当該復号ユニットAに固有のものであり、これを当該ユニットの中から何らかの手段で読み出したとしても他のユニットでは利用できないし、一定期間を過ぎれば無効になるように鍵保持部2005でスケジューリングすれば同じユニットでも一定期間を過ぎれば利用できなくなる。なお、鍵生成部2006は鍵保持部2005によって駆動される。

【0195】鍵保持部2005は予め定められたタイミングで鍵生成部2006に鍵生成の命令を送る。このタイミングは例えば図1の時計参照部2007で参照した時刻を基にする方法が一般的である。

【0196】図58は、鍵保持部2005、鍵生成部2006における鍵生成処理の概略手順を説明するためのフローチャートである。鍵保持部2005は、例えば、所定時間毎に時計参照部2007を介して時刻を参照し(ステップS1021)、予め定められた鍵の更新時刻であるときは、鍵生成部2006に対し鍵生成の命令を送り、鍵生成部2006では前述したような公開鍵および秘密鍵の生成を行う(ステップS1022〜ステップS1023)。現時刻が鍵更新時刻でないときは所定時間待つ(ステップS1025)。鍵生成部2006で生成された公開鍵および秘密鍵は鍵保持部2005に保持される(ステップS1024)。

【0197】このように鍵生成部2006にて鍵の何ども生成を行わなくとも、復号ユニットAを最初に使うときに初期化動作として一回鍵生成を行うだけでも、異なる復号ユニットAには異なる鍵が設定されることになり有効性は高い。もちろん、工場出荷時に別々の鍵を鍵保持部2005にセットすることも考えられる。この場合は鍵生成部2006は不要である。

【0198】本発明の復号ユニットAの特徴として、ライセンス情報を更新する際、鍵保持部2005が保持している公開鍵をライセンス情報を更新するために必要な他の情報とともにライセンス情報更新装置2008に送信する必要がある(この公開鍵は、ライセンス情報更新装置2008にて新たに生成された更新されたライセンス情報を暗号化する際に用いられるからである)。この手続きを行うのが更新情報生成部2004である。

【0199】更新情報生成部2004は、判定部2003でライセンス情報に基づきコンテンツの利用が不可と判定されたとき起動され、利用条件入力部2009を起動し、ユーザに対し、希望する利用条件(例えば、延長期間等)の入力を促す。これと並行して鍵保持部2005に公開鍵の出力を促し、得られた公開鍵と希望利用条件を判定部2003から送られるコンテンツIDなどの課金に必要な情報とともに予め定められたフォーマットに整理し、ライセンス情報を更新するための更新情報(図56参照)として、ライセンス情報更新装置2008に送る。

【0200】時計参照部2007は内部(場合によっては外部)にある時計2010を参照し、鍵保持部2005の鍵生成のタイミングを計るために用いるほか、利用条件の利用有効期限のチェックときにも用いられる。

## (2) 復号ユニットB

図59は、復号判定装置の他の構成例を示したものである。すなわち、復号ユニットBの構成例を示したもので、復号ユニット内で(一時的にでも)コンテンツ復号鍵が未暗号化データとして存在する状態を解消することができる。

【0201】コンテンツ復号鍵が当該ユニット内で未暗号化データとして存在すると当該ユニットを解析された

際、読み取られる危険性が生ずる。もし恒常的に読み取ることができれば、その方法を使ってあらゆるコンテンツ復号鍵は（復号ユニットが有する秘密鍵を知らなくても）取得できることを意味し、ライセンス保護の観点から重大なセキュリティホールとなる。この問題はその性質上秘密鍵を一定期間で生成し、古いものと置き換えるという前述の復号ユニットAの方法では解決できない。

【0202】復号ユニットB内では、コンテンツ復号鍵が暗号化されたままであり、当該復号ユニット内の情報だけでは暗号化されたコンテンツ復号鍵を復号できないような構成となっている。

【0203】図61に示すフローチャートを参照して、図59の復号ユニットBの各構成部の動作について説明する。

【0204】暗号化されたライセンス情報はライセンス情報入力部2001を通じて、復号ユニットBに入力し、例えば、復号部2002で復号ユニットB内に予め保持されている秘密鍵で復号される（ステップS1031～ステップS1032）。

【0205】図60は復号ユニットBに入力されるライセンス情報の一例を示す。図60に示すように、ライセンス情報には、少なくともコンテンツID、当該コンテンツの利用条件の他に、暗号化されたコンテンツ復号鍵 $[k_c] K_{AB}$ と、この暗号化されたコンテンツ復号鍵を復号するための共有鍵生成情報 $k_a$ とが含まれている。なお、コンテンツ復号鍵 $k_c$ は、共有鍵 $K_{AB}$ で暗号化されているものとする。さて、復号部2002で復号されたライセンス情報は、判定部2003へ送られ、ここで利用条件の判定が行われる（ステップS1933）。利用条件が満たされれば、暗号化されたコンテンツ復号鍵 $[k_c] K_{AB}$ と共有鍵生成情報 $k_a$ とが情報利用装置2020へ送られる（ステップS1034～ステップS1035）。

【0206】一方、判定部2003で利用不可と判定された場合は、更新情報生成部2004へライセンス更新に必要なコンテンツIDなどを送る（ステップS1034、ステップS1036）。

【0207】更新情報生成部2004は、共有鍵生成情報抽出部2031を介して当該コンテンツを利用する情報利用装置2020に対して、ライセンス情報更新装置2008においてコンテンツ復号鍵を暗号化するために必要な共有鍵生成情報 $k_b$ の出力を促す。

【0208】ここで、コンテンツ復号鍵を暗号化するための共有鍵生成情報 $k_a$ 、 $k_b$ について説明する。離散対数問題を安全性の根拠にした公開鍵暗号（例えば楕円曲線暗号）においては、以下のような共有鍵生成プロトコルが考えられる。まず情報利用装置2020とライセンス情報更新装置2008に共通な $x$ という元を予め決めておく。さらに、情報利用装置2020内に（例えば

出荷時に定めた）整数 $b$ と $x$ と $b$ から計算される元 $x^b$ とを予め求めて格納しておく。そしてライセンス更新の要求があった場合には、 $x^b$ を復号鍵生成情報 $k_b$ として復号ユニットBに送る。

【0209】復号ユニットBでは、利用条件入力部2009を介してユーザから入力された希望利用条件の他に復号鍵生成情報 $k_b$ とコンテンツIDとを含む更新情報（図62参照）を生成して、ライセンス情報更新装置2008に送る。

【0210】ライセンス情報更新装置2008では、乱数等を使って自ら決めた整数 $a$ を使って、復号ユニットBから送られてきた復号鍵生成情報 $k_b = x^b$ に対して、

$$(k_b)^a = x^{ab}$$

を計算し、これをコンテンツ復号鍵を復号する情報利用装置2020との間での共有鍵 $K_{AB}$ とする。

【0211】さらに、ライセンス情報更新装置2008は、更新したライセンス情報の中に図60に示したように、ライセンス情報更新装置2008自身が生成した共有鍵生成情報 $k_a$ 、すなわち $x^a$ を含める。そして、この更新されたライセンス情報は、復号部2002、判定部2003などを経て情報利用装置2020に送られる。

【0212】情報利用装置2020では、そこで予め保持されている各情報利用装置にユニークな整数 $b$ と、復号ユニットBから送られてきた復号鍵生成情報 $k_a$ とから、

$$(k_a)^b = (x^a)^b = x^{ab} = K_{AB}$$

という計算で共有鍵 $K_{AB}$ を得ることができる。

【0213】これにより、たとえ復号ユニットBの秘密鍵が読み取られても復号ユニットBの情報だけではコンテンツ復号鍵を得ることはできない。

【0214】何故ならば、共有鍵の生成情報として $k_a = x^a$ 、 $k_b = x^b$ が存在するが、これらから $K_{AB} = x^{ab}$ を構成することは計算量的に困難である。というのは、そのためにはどうしても整数 $a$ 、 $b$ をもとめる必要があるが、 $x^a$ と公開されている $x$ とから $a$ を求める問題は離散対数問題と呼ばれ、離散対数問題を安全性の根拠とする公開鍵暗号（例えば楕円曲線暗号）においては計算量的に困難であるからである。かくして、復号ユニットB内でコンテンツ復号鍵が未暗号化データとして存在する状態を解消することができ、復号ユニットB内部に存在する不可情報 $w$ 復号するための秘密鍵が読み出されてもコンテンツ復号鍵 $k_c$ が取り出せないシステムが実現した。

【0215】さて、図61の説明に戻り、ライセンス更新のため当該コンテンツを利用する情報利用装置2020は、共有鍵生成情報抽出部2031からの要求に応じて鍵生成情報 $k_b$ を出力し、共有鍵生成情報抽出部2031ではこれを受けて、更新情報生成部2004に鍵生

成情報k bを送る(ステップS1037)。これと並行して、共有鍵生成情報抽出部2031は利用条件入力部2009を起動し、ユーザに対して希望利用条件の入力を促し、更新情報生成部2004では、入力された希望利用条件と別途得られているコンテンツIDや鍵生成情報k bなどからライセンスの更新情報を生成して(図62参照)、例えば、所定の通信回線(インターネットでもよい)を経由してライセンス情報更新装置2008に送信する(ステップS1038～ステップS1040)。

【0216】なお、前述の公開鍵および秘密鍵を個別に保持もしくは生成する復号ユニットAの機能と、コンテンツ復号鍵をライセンス情報更新装置2008と情報利用装置2020との間の共有鍵で暗号化するように構成された復号ユニットBの機能とを組み合わせた復号ユニットCも構成できることは自明であろう。

【0217】この場合、復号ユニットCには、図60に示したようなライセンス情報が復号ユニットCから通知された公開鍵にて暗号化されたものが、図63に示したような復号ユニットCに入力する。なお、図63において、図54の復号ユニットAと同一部分は同一符号を付し、異なる部分は、更新情報生成部2004が、ライセンス更新の際に、情報利用装置2020に対しアクセスして、情報利用装置2020が保持する鍵生成情報k bを取得し、図64に示すような、少なくとも該取得された鍵生成情報k b、鍵生成部2006で生成された公開鍵、入力された希望利用条件、コンテンツIDを含むライセンスの更新情報を生成し、ライセンス情報更新装置2008に送信する点である。

### (3) 復号ユニットD

復号ユニットDは、前述の復号ユニットA、Bとは異なり、復号鍵がライセンス情報更新装置2008との間で1回限り利用される共有鍵である。すなわち、復号鍵は復号する際に、その都度生成し、復号ユニットD内に復号鍵を保持しなくても良い。これは秘密にするべき復号鍵が一時的に作られ、使われた後はすぐメモリ上から消去できることを意味し、復号ユニットの安全性向上の点から有効である。

【0218】図66は、復号ユニットDに入力されるライセンス情報の一例を示したもので、図66に示すように、暗号化部分と未暗号化部分で構成されている。暗号化部分は、少なくともコンテンツ利用条件、コンテンツ復号鍵k c、コンテンツIDからなっており、全体を復号ユニットDとライセンス情報更新装置2008との間の共有鍵 $K_{AB}$ で暗号化されている。未暗号化部分は、少なくとも共有鍵 $K_{AB}$ を生成するためにライセンス情報更新装置2008が生成した共有鍵生成情報k aと復号ユニットDが以下に述べる方法で生成する共有鍵生成情報k bから構成される。なお、共有鍵 $K_{AB}$ の生成方法は前述の復号ユニットBでの説明と同様である。

【0219】図65は、復号ユニットDの構成例を示したものである。図67に示すフローチャートを参照して、図65の復号ユニットDの各構成部の動作について説明する。

【0220】ライセンス情報はライセンス情報入力部2001を介して入力される(ステップS1051)。入力されたライセンス情報は、ライセンス情報入力部2001で暗号化部分と未暗号化部分とに分けられ、暗号化部分は復号部2002に送られ、未暗号化部分にある共有鍵生成情報k a、k bは、復号鍵生成部2041に送られる(ステップS10521)。

【0221】復号鍵生成部2041は、共有鍵生成情報k bを共有鍵生成情報生成部2042に送り、共有鍵生成情報生成部2042に格納されているテーブル2043を参照して、共有鍵生成情報k bに対応する共有鍵情報bを取得する(ステップS1053～ステップS54)。これを受けて復号鍵生成部2041は共有鍵生成情報k a、bとから共有鍵 $K_{AB}$ を生成する(ステップS1055)。

【0222】共有鍵 $K_{AB}$ は復号部2002に送られ、ライセンス情報の暗号化部分の復号に用いられる(ステップS1056)。

【0223】復号されたライセンス情報は判定部2003に送られ、ここで利用条件のチェックが行われる(ステップS1057)。その結果、コンテンツの利用が可能と判定された場合は、コンテンツ復号鍵k cを情報利用装置2020に出力する(ステップS1058～ステップS1059)。コンテンツの利用が不可と判定された場合、その旨を受けた更新情報生成部2004が共有鍵生成情報生成部2042に対し、共有鍵生成情報の生成を指示する。

【0224】共有鍵生成情報生成部2042では、これを受けて共有鍵情報bと共有鍵生成情報k bのペアを生成し、共有鍵生成情報生成部2042内部に具備されたメモリに格納されているテーブル2043に登録する(ステップS1060)。また、ここで生成された共有鍵生成情報k bは、更新情報生成部へ2004送られる。

【0225】一方、更新情報生成部2004は、希望利用条件の入力を利用条件入力部2009へ促し、利用条件入力部2004では然るべきヒューマンインタフェースを利用して、ユーザから希望利用条件の入力を受け、それを更新情報生成部2004に送る。

【0226】更新情報生成2004では、以上の過程で得られた情報を基に図69に示すような更新情報を生成し、所定の通信回線を介してライセンス情報更新装置2008に送信し、更新されたライセンス情報の発行を受けることになる(ステップS1061～ステップS1063)。

【0227】ライセンス情報更新装置2008では、前



述同様、共有鍵生成情報k aを生成するとともに共有鍵 $K_{AB}$ を生成して、図66の共有鍵生成情報k aを該生成された共有鍵生成情報k aに更新し、また、共有鍵生成情報k bを更新情報に含まれていた共有鍵生成情報k bに更新するとともに、更新情報に含まれていた希望利用条件に基づき更新された利用条件等を該生成された共有鍵 $K_{AB}$ で暗号化してライセンス情報を更新する。

【0228】さて、復号ユニットDでコンテンツを最初に利用再生する場合は、(共有鍵生成情報k bが生成されていないので)復号鍵生成部2041では、共有鍵 $K_{AB}$ が生成できない)のでライセンス情報を復号することができない(ステップS1053)。

【0229】この場合の処理について、図68に示すフローチャートを参照して説明する。この場合、当該ライセンス情報の未暗号化部分には、共有鍵生成情報k bが存在しない(もしくはNULLコードなどの無効な情報が入っている)ことで最初の利用再生であることを復号鍵生成部2041が検知し、共有鍵生成情報生成部2042に対し共有鍵生成情報を作成する旨の指示を行なう。これを受けて、共有鍵生成情報生成部2042では、共有鍵情報bと共有鍵生成情報k bのペアを生成し、共有鍵生成情報k bとライセンスを更新する旨の指示を更新情報生成部2004へ送る(ステップS1071)。

【0230】この場合、ライセンス情報の暗号化部分は(全ての復号ユニットDに共通に使われている)秘密鍵k sで暗号化されている。復号部2002では、復号鍵生成部2041からこの秘密鍵k sの出力を受け、暗号化部分を復号する(ステップS1072)。復号されたライセンス情報の暗号化部分からコンテンツIDを抽出する(ステップS1073)。

【0231】更新情報生成部2004では、これを受けて希望利用条件の入力を利用条件入力部2009へ促して、希望利用条件入力部2009を介してユーザからの希望利用条件の入力を受ける(ステップS1074)。更に以上の過程で得られたコンテンツID、希望利用条件と共有鍵生成情報k bを図69に示すような更新情報の予め定められたフォーマットにまとめ、これをライセンス情報更新装置2008に送信する(ステップS1075)。これにより更新されたライセンス情報が発行されることとなる。

【0232】このような最初の利用再生である場合は、ライセンス情報の暗号化部分に有効なコンテンツ復号鍵を入れないようにすると、さらに安全性が向上する。すなわち、もとのライセンス情報にコンテンツ復号鍵が含まれていなければ、例えば共通の秘密鍵k sが露見してもコンテンツ復号鍵は抽出できないので安全であるからである。この場合の暗号化は、コンテンツIDの変更を阻止するためのものであるといえる。

【0233】以上のようにすることによって、復号の度

に復号鍵 $K_{AB}$ を生成し、ライセンス情報が更新される度に異なる復号鍵 $K_{AB}$ で復号しなければならないので(ライセンス情報に含まれる復号鍵生成情報k bに応じてテーブル2043から検索された復号鍵情報bにて異なる復号鍵が生成されるので)、復号鍵 $K_{AB}$ が露見した場合の影響が少なくなる。そればかりか公開鍵暗号に比べ格段に高速である共有鍵暗号が使えるのでライセンス情報のデータサイズを大きくしても実時間で復号し、ライセンス情報に含まれる利用条件に基づくコンテンツの利用可否の反映が行えるという利点がある。

【0234】次に、復号ユニットDのバリエーションについて述べる。

【0235】まず、復号ユニットDが生成する共有鍵生成情報k bは固定であってもよい。この場合、安全性は少々落ちるが、ライセンス情報更新装置2008の作成する共有鍵生成情報k aが毎回変われば共有鍵 $K_{AB}$ は毎回変わるので、復号ユニットDの有効性は保たれる。また、図65に示す共有鍵生成情報生成部2042は不要となり、予め定められた共有鍵生成情報k b、共有鍵情報bを復号鍵生成部2041に持たせておけばよい。

【0236】また、復号ユニットDで最初にコンテンツ情報を利用再生する場合、図68に示したように、必ず共有鍵生成情報k bの取得に伴うライセンスの更新をしなければならないという問題があった。この問題を解決するために初回のライセンス情報に限っては、予め定められた共有鍵 $K_{com}$ か、公開鍵 $K_p$ で暗号化するという方法が考えられる。この場合、共有鍵 $K_{com}$ もしくは公開鍵 $K_p$ に対応する秘密鍵 $K_p$ を復号ユニットD内に保持している必要があり、初回だけそれを用いる。前述の図68に示した最初の利用再生時の処理動作と異なる点は、図68の場合、コンテンツ復号鍵を含めなくても良いが、今回の場合には必ず含めなくてはいけないという点である。

【0237】すなわち、図67のステップS1053において、復号鍵生成部2041で共有鍵生成情報k a、k bが存在しないことで、初回の利用再生であると判断し、復号鍵生成部2041もしくは復号部2002にある共有鍵 $K_{com}$ もしくは秘密鍵 $K_p$ を用いて復号部2002がライセンス情報を復号する。その後は、図67のステップS1054以降と同様である。

【0238】さらに、復号ユニットDが生成している共有鍵生成情報k bを情報利用装置2020に作らせる方法も考えられる。この場合の復号ユニットD'の構成を図70に示す。図70に示すように、図65の共有鍵生成情報生成部2042が情報利用装置2020に置き換わる。もっとも情報利用装置2020は、復号ユニットD'の外部にあるので共有鍵情報bは秘密にしなければならないが、これは復号鍵生成部2041と情報利用装置2020との間の一時鍵による暗号化によって解決できる。この場合、共通鍵情報bですら復号ユニットD'

内に保持しないことになり、復号ユニットDより安全になる。しかし、このような場合は情報利用装置2020の方も攻撃の対象になるが、それは情報利用装置個々によって実装の仕方が違うので個別の対応が必要であり、情報利用装置2020によって安全性のレベルを変えることもできる。尚、復号ユニットD'の処理動作は、図67、図68に示したフローチャートと同様である。

(4) 復号ユニットAに対応するライセンス情報更新装置図71は、前述の復号ユニットAに対応するライセンス情報更新装置2008の構成例を示したものである。以下、図72に示すフローチャートを参照して、図71のライセンス情報更新装置2008の各構成部の処理動作について説明する。

【0239】復号ユニットAから送信されるライセンスの更新情報は、更新情報入力部2051を介しライセンス情報更新装置2008に入力する(ステップS1081)。

【0240】ここで用いられる更新情報は、図56に示した更新情報で、希望利用条件、コンテンツID、復号ユニットAで生成された公開鍵などが含まれた、ライセンスの更新に必要な情報である。この中で、コンテンツIDは利用許可を与えるコンテンツを特定するためのものであり、これによってライセンス情報更新装置2008の持つデータベースを使って希望利用条件にあった課金情報が取得でき、更に当該コンテンツ復号鍵もデータベースを使って取得できるのである。このためライセンス情報更新装置2008には、ライセンス情報を更新するためにコンテンツ復号鍵を入力する必要はなく、従って図56の更新情報は暗号化して送る必要もない。この点も図72に示したライセンス情報更新装置2008の特徴である。

【0241】さて、更新情報入力部2051から入力した図56に示したような更新情報は、料支払要求部2052に送られ、ここから、更新情報に含まれている希望利用条件が料金問い合わせ部2057に送られる。

【0242】料金問い合わせ部2057では、料金データベース(DB)2058にアクセスして、希望利用条件に対応した料金を取得する(ステップS1082～ステップS1083)。例えば、希望利用条件として2ヶ月という有効期間が指定されていたら、その期間に見合ったコンテンツIDのコンテンツの利用料金値が検索されて、料金問い合わせ部2057、さらに、料金支払要求部2052に渡される。

【0243】料金支払要求部2052は、取得した料金値と更新情報に含まれる当該顧客に関するデータとを基に、所定の通信回線を介して所定の電子決済システム2060にアクセスして当該顧客からの料金の支払要求を行う。電子決済システム2060は、所定の電子支払処理を実行する(ステップS1084)。

【0244】ライセンス情報更新装置2008の支払い

確認部2053は、所定の通信回線を介して、電子決済システム2060と交信して、料金の支払いが確認されると、次に、コンテンツ復号鍵取得部2054での処理に以降する(ステップS1085)。

【0245】コンテンツ復号鍵取得部2054では、コンテンツIDをキーにしてコンテンツ復号鍵データベース(DB)2059を検索し、コンテンツ復号鍵を取得する(ステップS1086)。なお、ライセンス情報更新装置2008は、特定の信頼できる業者が管理運営していると考えているので、コンテンツ復号鍵DB2059内も得られたコンテンツ復号鍵も特に暗号化する必要はない。

【0246】次に、ライセンス情報暗号化部2055では、上記得られた情報を基にライセンス情報を構築し(ステップS1087)、そのライセンス情報を、先に受け取った図56に示したような更新情報に含まれている公開鍵で暗号化し(ステップS1088)、ライセンス情報出力部2056を介して、ライセンス情報の更新要求元のクライアント、すなわち、復号ユニットAに所定の通信回線を介して送信する(ステップS1089)。(5) 復号ユニットBに対応するライセンス情報更新装置図73は、前述の復号ユニットBに対応するライセンス情報更新装置2008の構成例を示したものである。以下、図74に示すフローチャートを参照して、図73のライセンス情報更新装置2008の各構成部の処理動作について説明する。

【0247】なお、図73において、図71と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図73において、コンテンツ復号鍵取得部2054とライセンス情報暗号化部2055との間に共有鍵生成部2061とコンテンツ復号鍵暗号化部2062とが追加されている。また、図74のフローチャートにおいて、図72のフローチャートと同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、ステップS1086とステップS1087の間に、共有鍵生成部2061にて整数aと共有鍵生成情報kaとを生成して、これらと更新情報に含まれる各情報利用装置2020にユニークな共有鍵生成情報kbとから共有鍵 $K_{AB}$ を生成し(ステップS1091～ステップS1092)、さらに、暗号化部2062で、この新たに生成された共有鍵 $K_{AB}$ を用いてステップS1086で新たに取得されたコンテンツ復号鍵を暗号化する処理(ステップS1093)が追加される。

【0248】図73の構成では、コンテンツ復号鍵を暗号化してライセンス情報に入れるために共有鍵生成部2061において、情報利用装置2020とライセンス情報更新装置2008との間で該暗号化されたコンテンツ復号鍵を復号するための共有鍵を生成する必要がある。共有鍵の生成法は復号ユニットBの説明でも述べたように共有鍵生成情報を用いて行う。従って、図73のライ

センス情報更新装置2008に入力される更新情報は、図62のように、少なくとも希望利用条件とコンテンツIDと情報利用装置2020が乱数等を使って生成した共有鍵生成情報k bが含まれている。

【0249】ステップS1088では、ライセンス情報暗号部2055にて新たに生成されたライセンス情報が予め定められた公開鍵で暗号化される。

【0250】なお、前述の公開鍵および秘密鍵を個別に保持もしくは生成する復号ユニットAの機能と、コンテンツ復号鍵をライセンス情報更新装置2008と情報利用装置2020との間の共有鍵で暗号化するように構成された復号ユニットBの機能とを組み合わせた復号ユニットCに対応するライセンス情報更新装置の場合、入力される更新情報には、さらに復号ユニットCで生成された公開鍵を含み、図74のステップS1088では、当該公開鍵を用いて生成されたライセンス情報を暗号化すればよい。

【0251】また、復号ユニットD、D'に対応するライセンス情報更新装置も図73とほぼ同様で、異なるのは、図73の暗号化部2062では、利用条件とコンテンツ復号鍵k c、コンテンツIDとを共有鍵K<sub>AB</sub>を用いて暗号化し、図66に示したようなライセンス情報を生成し、その生成されたライセンス情報は、そのままライセンス情報出力部2050を介して出力されることである。

(第3の実施形態)第3の実施形態に係る情報流通システムの構成例を図75に示す。

【0252】図75において、利用者はDVD等のリムーバブル情報蓄積メディア(以下、簡単にメディアと呼ぶ)に記録された課金対象であるコンテンツ情報を入手する。当該コンテンツ情報に対するライセンス情報もまた当該メディアに記録されている。利用者の情報再生装置には、復号ユニットが内蔵され、メディアから読み出されたライセンス情報に基づき当該コンテンツ利用の可否を判定するようになっている。

【0253】コンテンツ利用が不可の場合に、利用者が当該コンテンツを利用するためには、ライセンス情報の更新を受けなければならない。すなわち、コンテンツの利用が可能となるように、ライセンス情報に含まれる利用条件を更新、すなわち、ライセンスの更新を行う必要がある。この利用条件、ひいてはライセンス情報の更新を行うのは、例えば、そのためのライセンス更新端末を有する店舗で行われる。ライセンス更新端末はライセンス販売代行業者が運営するライセンスサーバに接続されている。利用者は所望の利用条件(例えば、コンテンツの指定とその利用期間等)を指定して、それに応じたライセンス料金(利用条件に見合うコンテンツの利用料金)を店舗に支払う。すると、ライセンス更新端末はライセンスサーバと通信して、ライセンスサーバから送られてくる情報に基づきメディアに記録されているライセ

ンス情報が更新されることにより、ライセンスが更新される。例えば、利用者が期限付きライセンスを購入した場合、利用期限満了迄ライセンス更新を行うことなくコンテンツを利用する事ができる。

【0254】図76は、情報流通システムの他の構成例を示したものである。図75と異なる点は、少なくとも復号ユニットの機能がICカード等のカード型の記録媒体に内蔵されている。以下、復号ユニットを内蔵したICカード等のカード型記録媒体を復号判定カードと呼ぶ。この場合、利用者はライセンスを更新する際、復号判定カードをライセンス更新端末を有する店舗に携帯する。ライセンス更新端末は復号判定カードから公開マスターキーを読み取り、ライセンスサーバに転送する。利用者は所望の利用条件(例えば、コンテンツの指定とその利用期間等)を指定して、それに応じたライセンス料金(利用条件に見合うコンテンツの利用料金)を店舗に支払う。すると、ライセンス更新端末はライセンスサーバと通信して、ライセンスサーバから送られてくる情報に基づきメディアに記録されているライセンス情報が更新され、ライセンスが更新される。

【0255】なお、公開マスターキーについては後述する。

【0256】また、図75において、復号ユニットは、情報再生装置に内蔵されている場合にのみ限らず、図76の復号判定カードのような形態であって、情報再生装置に着脱可能に装着されていてもよく、以下、図75、図76の情報流通システムについて、復号判定カードを用いる場合を例にとり説明する。

(1) 以下、図75の情報流通システムについて説明する。

#### (1-1) 情報再生装置

図77は、復号判定カードを装着した情報再生装置の要部の構成例を示したもので、バス3007に復号判定カード3001、メディア読取装置3003、情報再生装置3004、時計3005、中央処理装置3006が接続されて構成されている。

【0257】時計3005は、利用条件としてのコンテンツの利用期限を有効/無効を判定するためのもので、前述の第1の実施形態で説明したように、暗号化コマンドによる時刻設定を行うことを特徴としている。ライセンス更新の際には、この時計の時刻をサーバの時刻に合わせる、時刻設定動作を行う。この動作については、前述した通りである。これによって、時計3005の時刻をほぼ正確に維持する事が可能となる。

【0258】メディア読取装置3003は、DVD等のメディア3002に記録された情報を読み取り、この読み取られた情報に基づき復号判定装置3001でメディア3002に記録されたコンテンツ情報の利用の可否を判定し、利用可と判定された場合は情報再生部3004は、メディア読取装置3003でメディア3002から

読み取られたコンテンツ情報を再生できるようになっている。中央処理装置3006は上記各部の動作を制御するためのものである。

【0259】図77の復号判定カード3001と時計3005とは、それぞれ鍵生成情報K<sub>t</sub>を保持している。また、復号判定カード3001と情報再生装置3004とは、それぞれ鍵生成情報K'を保持している。

【0260】乱数A、Bおよび鍵生成情報K<sub>t</sub>に基づき、時計3005と復号判定カード3001との間で現在時刻情報を転送する際に該情報の暗号化／復号化のために1回限り有効な転送キーKTが生成される。また、乱数C、Dおよび鍵生成情報K'に基づき、復号判定カード3001と情報再生部3004との間で暗号化されたコンテンツ情報を復号するコンテンツキーK<sub>c</sub>を転送する際に、該コンテンツキーK<sub>c</sub>の暗号化／復号化のために1回限り有効な転送キーKTが生成される。これによって、バス3007を流れる情報データが保護される。

【0261】メディア3002には、次の様な情報が格納されている。

- ・マスターキーKMによって暗号化されたライセンス情報（[ライセンス情報]KM）
- ・ライセンス情報を復号するためのマスターキーKMを指定する識別子（例えば、番号）であるマスターキーID
- ・コンテンツキーK<sub>c</sub>によって暗号化されたコンテンツ情報（[コンテンツ]K<sub>c</sub>）

なお、以下の説明では、ライセンス情報を暗号化／復号化の際に用いる暗号キーと復号キーとを合わせてマスターキーKMと呼び、ライセンス情報の暗号キーと復号キーとが必ずしも同じキーであるとは限らない。

【0262】ライセンス情報は、次の様な情報から構成されている。

- ・コンテンツキーK<sub>c</sub>
- ・コンテンツID
- ・利用期限、利用開始時刻、及びライセンス情報記録時刻等のコンテンツの利用条件

図78に示すフローチャートは、図75の情報流通システムで用いられる図77の情報再生装置の処理動作を示したものである。

【0263】まず、メディア読取装置3003は、そこにセットされたメディア3002からマスターキーID、[ライセンス情報]KMを読み取り、復号判定カード3001に、それらを転送する（ステップS3001～ステップS3002）。

【0264】時計3005は、所定のアルゴリズムにて乱数Aを発生して、それを復号判定カード3001に転送する（ステップS3003）。一方、復号判定カード3001も所定のアルゴリズムにて乱数Bを発生し、時計3005に転送する（ステップS3004）。これに

より、復号判定カード3001と時計3005は互いに乱数A、Bを確認し合うこととなる。

【0265】復号判定カード3001および時計3005は、乱数A、B、および自らが保持している鍵生成情報K<sub>t</sub>から転送キーKTを生成する（ステップS3005、ステップS3006）。時計3005は生成された転送キーKTで、現在の時刻情報を暗号化し（[現在時刻]KT）、それを復号判定カード3001へ転送する（ステップS3007）。

【0266】復号判定カード3001では、[ライセンス情報]KMをマスターキーIDにて指定されたマスターキーKMを用いてライセンス情報を復号し、また、時計3005から転送されてきた[現在時刻]KTを生成された転送キーKTで復号し、復号されたライセンス情報と復号された時刻情報とに基づき、コンテンツIDにて指定されるコンテンツ情報の利用の可否、すなわち、復号の可否を判定する（ステップS3008）。復号が不可と判定されたときは、処理を終了する。

【0267】復号が可能と判定されたときは（ステップS3009）、復号判定カード3001は所定のアルゴリズムにて乱数Cを発生し、それを情報再生部3004に転送する（ステップS3010）。情報再生部3004も所定のアルゴリズムにて乱数Dを発生する（ステップS3011）。これにより、復号判定カード3001と情報再生部3004は互いに乱数C、Dを確認し合うこととなる。

【0268】復号判定カード3001および情報再生部3004は、乱数C、D、および自らが保持している鍵生成情報K'から転送キーK'Tを生成する（ステップS3012、ステップS3013）。復号判定カード3001は、生成された転送キーK'Tでライセンス情報に含まれていたコンテンツキーK<sub>c</sub>を暗号化して（[K<sub>c</sub>]K'T）、それを情報再生部3004へ転送する（ステップS3014）。

【0269】メディア読取装置3003は、メディア3002から[コンテンツ]K<sub>c</sub>を読み取り、それを情報再生部3004へ転送する（ステップS3015）。

【0270】情報再生部3004は、[K<sub>c</sub>]K'Tを生成された転送キーK'Tで復号し、その結果得られたコンテンツキーK<sub>c</sub>でコンテンツ情報を復号する（ステップS3016）。

（1-2）復号判定カード

図79は、復号判定カード3001の構成例を示したものである。

【0271】時刻転送部3012は、図77の情報再生装置に具備される時計3005でカウントされている時刻情報を受け取り、復号判定部3013に転送するためのものである。

【0272】コンテンツキー転送部3014は、図77の情報再生部3004へのコンテンツキーK<sub>c</sub>の転送保

護の為の動作を行う。

【0273】データ転送部3011は、時計3005から転送される時刻情報、情報再生部3004へ転送するコンテンツキー以外の情報を、メディア読取装置3003、情報再生部3004、復号判定カード3001との間でやりとりする際に用いられる。

【0274】時刻転送部3012とデータ転送部3011とを別個に設けるのは、時刻転送に伴って、一時キーによるデータ保護とクロックによるタイムアウトなど特別な処理が行われる為である。

【0275】図80に示すフローチャートは、図79の復号判定カード3001における、コンテンツ情報の利用可否の判定結果を出力するまでの処理動作をより詳細に示したものである。

【0276】図78のステップS3002でメディア読取装置3003から転送されたマスターキーID、[ライセンス情報]KMは、データ転送部3011を介して復号判定部3013に入力する(ステップS3021)。また、図78のステップS3003で時計3005から転送された乱数Aは、時刻転送部3012に入力する(ステップS3022)。これを受けて、時刻転送部3022は、乱数Bを発生し、この乱数Bと先に受け取った乱数Aとから転送キーKTを生成する(ステップS3023～ステップS3024)。乱数Bを時計3005に転送する(ステップS3025)。これと同時に、時刻転送部3022は、クロックカウンタのカウンタを開始する(ステップS3026)。

【0277】図78のステップS3007で時計3005から転送された[現在時刻]KTは時刻転送部3022に入力したとき(ステップS3027)、時刻転送部3022のカウンタ値が予め定められた値Ct以内でないときは処理を終了する(ステップS3028)カウンタ値Ctは、タイムアウト時間で、予め定められた正整数である。本実施形態の場合、復号判定カードは時刻情報を復号判定カード3001の外部から取得する。従って、取得した時刻情報の正当性が問題になる。時計3005と復号判定カード3001の時刻転送部3012との間で乱数A、Bを交換し、一度限り有効な鍵KTで時刻情報を暗号化して転送するのは、その為である。しかし、それだけでは、時刻情報の転送を意図的に遅延させるという不正に対して対処できない。

【0278】そこで、時刻転送部3012は、時刻情報の到着時間、すなわち、時刻転送部3012が乱数Bを出力してから(暗号化された)時刻情報が時刻到着部3012に到着するまでの時間が、一定の時間Ct以内でなければ処理を停止することによって、この種の不正を防ぐことができる。

【0279】[現在時刻]KTの入力が所定時間以内であれば、それを先に生成された転送キーKTで復号して時刻情報を得る(ステップS3029)。時刻情報は復

号判定部3013に転送され、復号判定部3013では、復号されたライセンス情報と復号された時刻情報とに基づき、コンテンツIDにて指定されるコンテンツ情報の利用可否、すなわち、復号の可否を判定する(ステップS3031)。復号が不可と判定されたときは、処理を終了する。

【0280】復号が可能と判定されたときは(ステップS3032)、復号判定部3013はライセンス情報に含まれていたコンテンツキーkcをコンテンツキー転送部3014に出力する(ステップS3033)。

【0281】コンテンツキー転送部3014は乱数Cを発生すると、それを情報再生部3004に転送する(ステップS3034)。そして、図78のステップS3011で情報再生部3004から転送された乱数Dがコンテンツキー転送部3014に入力すると、この乱数Dと乱数Cとから転送キーK'Tを生成する(ステップS3035～ステップS3036)。コンテンツキー転送部3014は、生成された転送キーK'Tを用いてコンテンツキーKcを暗号化して([Kc]K'T)、それを情報再生装置3004へ転送する(ステップS3038)。

(1-3) 復号判定カードの時刻転送部

次に、図79の時刻転送部3012についてより詳細に説明する。図81は、時刻転送部3012の構成例を示したもので、認証部3021とクロックカウンタ3023と時刻出力部3022とから構成されている。

【0282】図81において、クロックカウンタ3023は、ロジック駆動用のクロックを数える計数カウンタである。

【0283】図82は、図81の認証部3021の構成例を示したものである。

【0284】図82において、秘密鍵格納部3021eは、鍵生成情報Ktを保持している。

【0285】転送鍵生成部3021fは適当なアルゴリズムによって、乱数A、B及び鍵生成情報Ktから、秘密鍵としての転送キーKTを生成する。このアルゴリズムは、対応する時計3005の認証部における秘密鍵生成アルゴリズムと同一であり、従って、復号判定カード3001と時計3005は転送キーKTを共有することができる。

【0286】予め定められたカウンタ値Ctは入出力部3021aが保持しており、クロックカウンタ3023の値を参照してタイムアウトを判定する。Ctの値には、時計3005が乱数Bを受け取ってから暗号化した時刻情報を返す迄に必要なクロック数に、転送の為の若干の余裕を持たせた値を設定する。

【0287】図83は、図82に示した認証部の処理動作を説明するためのフローチャートである。

【0288】図80のステップS3022で時刻転送部3012に入力された乱数Aは、まず、認証部3021

の入出力部3021aに入力し(ステップS3041)、乱数Aは乱数格納部3021bに格納される(ステップS3042)。次に、乱数発生部3021cは、所定のアルゴリズムにて乱数Bを発生し(ステップS3042)、乱数格納部3021dに格納するとともに、乱数Bを入出力部3021aに転送する(ステップS3045)。

【0289】転送鍵生成部3021fは、乱数格納部3021b、3021dのそれぞれに格納された乱数A、Bと、秘密鍵格納部3021eに格納されている鍵生成情報k<sub>t</sub>とを読み出して転送キーKTを生成し(ステップS3046)、転送鍵格納部3021gに格納する(ステップS3047)。

【0290】入出力部3021aはクロックカウンタ3023をリセットするとともに乱数Bを時計3005に転送する(ステップS3048～ステップS49)。

【0291】図80のステップS3027で時刻転送部3012に入力された[現在時刻]KTは、まず、入出力部3021aに入力する(ステップS3050)。入出力部3021aはクロックカウンタ3023のカウント値を読み出し、C<sub>t</sub>と比較し、カウント値がC<sub>t</sub>以下のときはステップS3053に進み、C<sub>t</sub>を越えているとき(タイムアウト時)は処理を終了する(ステップS3051～ステップS3052)。

【0292】ステップS3053では、[現在時刻]KTを復号部3021hに転送し、復号部3021hは転送鍵格納部3021gから転送キーKTを読み出して、転送キーKTで[現在時刻]KTを復号し、現在時刻情報を得る(ステップS3053～ステップS3054)。

【0293】データ形式確認部3021iは、現在時刻情報のデータ形式を確認する(ステップS3055)。現在時刻情報のデータ形式は、例えば、次のようなものである。

【0294】「現在時刻」/現在時刻/「00000000」「現在時刻」という文字列に続き、文字列で表現された現在時刻、最後の1バイトのデータ「0」は区切り記号である。現在時刻は、西暦1998年1月1日午前零時からの経過時間を分単位で表したものとす。

【0295】データ形式確認部3021iは、現在時刻情報のデータ形式が上記のような予め定められた形式を満足している場合のみ、該現在時刻情報を時刻出力部3022に出力する(ステップS3056)。

【0296】時刻出力部3022は、時刻情報を復号判定部3013に出力する(図80のステップS3030)。

【0297】なお、現在時刻情報の転送の際には、暗号化用のキーと復号用のキーが同一(KT)である様な暗号化方式を採用したが、この場合に限らず、異なるキーを用いるようにしても、上記同様の構成および動作で転

送保護を実現することができる。

(1-4) 復号判定部のコンテンツキー転送部

次に、図79のコンテンツキー転送部3014についてより詳細に説明する。図84は、コンテンツキー転送部3014の構成例を示したもので、認証部3031とコンテンツキー入力部3032とから構成されている。

【0298】図85は、認証部3031の構成例を示したもので、図86に示すフローチャートを参照して、認証部3031の処理動作について説明する。

【0299】乱数発生部3031cは、例えば所定のアルゴリズムにて乱数Cを発生して、乱数Cを乱数格納部3031dに格納すると同時に(ステップS3061)、入出力部3031aを介して情報再生部3004に転送される(ステップS3062)。

【0300】情報再生部3004から転送されてきた乱数Dが入出力部3031aを介して入力すると乱数格納部3031bに格納される(ステップS3064)。

【0301】転送鍵生成部3031fは、乱数格納部3031b、3031dのそれぞれに格納されている乱数C、Dと、秘密鍵格納部3031eに格納されている鍵生成情報K'<sub>t</sub>とを読み出して転送キーK'Tを生成し、それを転送鍵格納部3031gに格納する(ステップS3065～ステップS3066)。

【0302】図80のステップS3032にて、復号判定部3013における復号判定の結果、復号可と判定された場合、復号判定部3013は、コンテンツキーK<sub>c</sub>をコンテンツキー転送部3014に転送する(図80のステップS3033)。このコンテンツキーK<sub>c</sub>は、図85の暗号化部3031hに入力し、さらに、暗号化部3031hは、転送鍵格納部3031gから転送キーK'Tを読み出して、これを用いてコンテンツキーK<sub>c</sub>を暗号化し([K<sub>c</sub>]K'T)、入出力部3031aを介して情報再生部3004に転送する(ステップS3069)。

(1-5) 時計

図87は、図77の時計3005の構成例を示したもので、認証部3041、時計カウンタ3042とから構成される。

【0303】時計カウンタ3042は時刻をカウントするためのものである。

【0304】図88は、時計3005の認証部3041の構成例を示したものである。ここで、図89に示すフローチャートを参照して認証部3041の処理動作について説明する。

【0305】乱数発生部3041cは、所定のアルゴリズムにて乱数Aを発生し、乱数Aを乱数格納部3041dに格納するとともに(ステップS3071)、入出力部3041aを介して復号判定カード3001に転送する(ステップS3072)。入出力部3041aに復号判定カード3001から転送されてきた乱数Bが入力す

ると、乱数Bは乱数格納部3041dに格納される（ステップS3073）。

【0306】転送鍵生成部3041fは、乱数格納部3041b、3041dから乱数B、乱数Aをそれぞれ読み出し、また、秘密鍵格納部3041eから鍵生成情報K' tを読み出して、転送キーK' Tを生成し、それを転送鍵格納部3041gに格納する（ステップS3074～ステップS75）。

【0307】時計カウンタ3042から出力される現在時刻情報は暗号化部3041hに入力する（ステップS3076）。

【0308】暗号化部3041hは転送鍵格納部3041gから転送キーK' Tを読み出し、この転送キーK' Tで現在時刻情報を暗号化し（〔現在時刻〕K' T）、入出力部3041aを介して復号判定カード3001に転送する（ステップS3077～ステップS3078）。

（1-6）復号判定カードの復号判定部

図90に図79の復号判定カード3001の復号判定部3013の構成例を示す。

【0309】図91に示すフローチャートを参照して図90の復号判定部3013の処理動作について説明する。

【0310】メディア読取装置3003から復号判定カード3001に転送されたマスターキーID、〔ライセンス情報〕KMは、それぞれマスターキー選択部3061、復号部3063に入力される（ステップS3101、ステップS3103）。

【0311】マスターキー選択部3061はマスターキーIDに対応する復号キーをマスターキー格納部3062を検索して取得し、それを復号部3063に転送する（ステップS3102）。

【0312】マスターキー選択部3061に入力するマスターキーIDは〔ライセンス情報〕KMを暗号化しているキーに対応する復号キーを指定するためのものである。正しいマスターキーIDがなければ、ライセンス情報を復号する復号キーを選択することができない。

【0313】復号部3063は〔ライセンス情報〕KMをマスターキーIDにて指定された復号キーで復号し、その結果得られたライセンス情報を判定部3064に転送する（ステップS3105）。

【0314】判定部3064には、時計3005から復号判定カード3001の時刻転送部3012へ転送されて、ここで復号されて得られた現在時刻情報が時刻入力部3065を介して入力する（ステップS3106～ステップS3107）。

【0315】判定部3064では、ライセンス情報と現在時刻情報とに基づきコンテンツ情報の利用可否、すなわち復号可否を判定し、判定結果出力部3066を介して判定結果をデータ転送部3011に出力する（ステッ

プS3108～ステップS3110）。また、復号可と判定されたときは、ライセンス情報に含まれているコンテンツキーKcをコンテンツ出力部3067を介してコンテンツキー転送部3014に出力する（ステップS3111）。

【0316】ここで、判定部3064の判定処理について説明する。時計3005から送られる現在時刻がライセンス情報のメディア3002への記録時刻以前であれば、それは、現在時刻が正しい時刻から遅れている事を示す。ライセンス情報記録時刻はライセンスサーバーが記録しており、従って、ほぼ正確な時刻であると考えて良いからである。従って、この場合、判定部3064が具備する判定フラグをクリアして、以後全ての判定を「利用不可」とする。判定フラグを再びセットして判定を有効にするには、情報再生装置の時計3005からのコマンドを要する。このコマンドは、復号判定カード3001の時刻転送部3012を経由して復号判定部3013に送られる。従って、正統な（認証可能な）時計3005からのコマンドのみが、判定フラグを再設定できる。そして、時計3005が判定フラグを再設定するのは、時計3005の時刻が設定されたときのみである。

（1-7）マスターキー

ライセンス情報を暗号化、復号化する際に用いるマスターキーについて説明する。なお、ここでは、ライセンス情報を暗号化／復号化の際に用いる暗号キーと復号キーとを合わせてマスターキーと呼び、ライセンス情報の暗号キーと復号キーとが必ずしも同じキーであるとは限らない。

【0317】図90のマスターキー格納部3062におけるマスターキーは、マスターキーIDとともに、例えば、次のように記憶されている。Km(0)、…、Km(999)、(KP(1000)、Ks(1000))、…、(KP(1499)、Ks(1499))、(KP(1500)、Ks(1500))、…、(KP(1599)、Ks(1599))

Km(0)からKm(999)迄の1000個のキーは予め定められた復号用の秘密鍵である。KP(1000)からKP(1599)は、ライセンス情報暗号化用の公開鍵であり、Ks(1000)からKs(1599)の600個のキーはKP(1000)からKP(1599)のそれぞれのライセンス情報復号用の秘密鍵である。KP(n) (1000 ≤ n < 1600) を公開マスターキーと呼ぶ。

【0318】1000以上1600未満の任意のnについて、KP(n)とKs(n)とは対になるキーである。即ち、KP(n)で暗号化されたライセンス情報はKs(n)によって復号できる。1000以上1600未満の各nについて、(KP(n)、Ks(n))の対は、図90のマスターキー生成部3069によって、乱数発生部3068で発生される乱数に基づき随時生成さ

れる。従って、復号判定カード毎に異なっているばかりで無く、同じ復号判定カードでも時期によって異なっている。

【0319】公開マスターキーは、後述するように、図76の情報流通システムで用いられる。

【0320】 $(K_P(n), K_S(n))$  ( $1500 \leq n < 1600$ ) のキーを、コンテンツ情報を利用できる有効期間が例えば100時間未満の場合に用いるようにしてもよい。すなわち、マスターキー生成部3069は例えば1時間毎にキーの対を生成し、 $n=1500$  から  $n=1599$  に順次記録して行く。指定された有効期間に於いて、例えば有効期間が最長の100時間未満の場合 ( $K_P(1599n), K_S(1599)$ ) を記録した後は再び ( $K_P(1500), K_S(1500)$ ) を上書きし、以後これを繰り返す。

【0321】このようなマスターキー ( $(K_P(n), K_S(n))$  ( $1500 \leq n < 1600$ ) のキー) を用いる場合、ライセンス情報の暗号化には、常に最新の  $K_P(n)$  を用いる。ライセンス情報記録後、最長で99時間までは、 $K_P(n)$  で暗号化されたライセンス情報は対応する  $K_S(n)$  で復号されるが、100時間以上の時間が経過すると、 $K_S(n)$  が失われてしまう (上書きにより変更されてしまう) 為、このライセンス情報を復号する事はもはや不可能になる。これによって、高いセキュリティを確保する事が可能である。たとえば、何らかの方法でマスターキー  $K_S(n)$  を読み取った者がいたとしても、このキーは特定の1時間の間に作成されたライセンス情報に対してのみ、有効である。

【0322】以上の様に、マスターキー格納部3062がそれぞれ性質の異なる3種類のマスターキー (すなわち、全ての復号判定カードで共通の秘密鍵、各復号判定カードでユニークな秘密鍵、各復号判定カードで所定時間毎に更新される秘密鍵) を保持することによって、セキュリティと利便性のカスタマイズが可能となる。

【0323】 $K_m(0)$  から  $K_m(999)$  にそれぞれ対応する暗号キー  $K_M(0)$ 、…、 $K_M(999)$  で暗号化されたライセンス情報は、どの復号判定カードによっても復号判定に使用することができる。しかし、万が一復号判定カードの内容が盗み取られた場合、コンテンツの保護が破綻してしまうというリスクが伴う。

【0324】一方、公開マスターキーによる方法は、ライセンス情報更新の際、公開マスターキーをサーバーに送る必要がある。従って、利用者に余分な手間を強いる場合もある。しかし、復号判定カードの内容が盗み読まれた場合にも、セキュリティの破綻は特定の復号判定カードに限定される。特に、上述の様な時変方式の公開マスターキーを使用した場合、セキュリティの破綻は時間的にも限定される。

(1-8) 情報再生部

図92は、図77の情報再生部3004の構成例を示し

たもので、認証部3051、復号部3052、デコーダ3053、D/A変換部3054から構成されている。

【0325】図93に示すフローチャートを参照して図92の情報再生部3004の処理動作の概略を説明する。情報再生部3004は例えばMPEG2等の動画再生を行う。

【0326】復号判定カード3001から転送された暗号化されたコンテンツキー  $[K_c] K' T$  は、情報再生部3004の認証部3051に入力する。認証部3051は自らが生成した転送キー  $K' T$  を用いて  $[K_c]$   $K' T$  を復号し、コンテンツキー  $K_c$  を得る (ステップS3081)。

【0327】一方、復号部3052には、メディア読取装置3003でメディア3002から読み取られたコンテンツキー  $K_c$  で暗号化されたコンテンツ情報が入力する。復号部3052は、コンテンツキー  $K_c$  でコンテンツ情報を復号しデコーダ3053に出力する (ステップS3082)。

【0328】デコーダ3053は、圧縮の為に施されたコーディングを復元し、その結果得られた画像データ等をD/A変換部3054に送る (ステップS3083)。

【0329】D/A変換部3054は、これをアナログ信号に変換し、所定の表示装置に出力する (ステップS3085)。

【0330】図94は、図92の情報再生部3004の認証部3051の構成例を示したものである。図95に示すフローチャートを参照して認証部3051の処理動作について説明する。

【0331】復号判定カード3001から情報再生部3004に転送された乱数  $C$  は、認証部3051の入出力部3051aに入力し、乱数格納部3051bに格納される (ステップS3091)。

【0332】乱数発生部3051cは乱数  $D$  を発生し、乱数格納部3051dに格納する (ステップS3092)。

【0333】転送鍵生成部3051fは、乱数格納部3051b、3051dからそれぞれ乱数  $C$ 、乱数  $D$  を読み出し、また、秘密鍵格納部3051eから鍵生成情報  $K' t$  を読み出して、転送キー  $K' T$  を生成する (ステップS3093)。この生成された転送キー  $K' T$  は転送鍵格納部3051gに格納される (ステップS3094)。

【0334】乱数格納部3051dに格納された乱数  $D$  は、また、入出力部3051aを介して復号判定ユニット3001へ転送される (ステップS3095)。

【0335】復号判定カード3001から情報再生部3004に転送された暗号化されたコンテンツキー  $[K_c] K' T$  は、認証部3051の入出力部3051aに入力する。  $[K_c] K' T$  は復号部3051hに出力さ



れる(ステップS3096)。復号部3051hは、転送鍵格納部3051gから転送キーK'Tを読み出して[Kc]K'Tを復号し、コンテンツキーKcを得る(ステップS3097)。コンテンツキーKcは情報再生部3004内の復号部3052に出力される(ステップS3098)。

#### (1-9) 他の情報再生部

図96は、図77の情報再生部3004の他の構成例を示したもので、課金対象のコンテンツ情報がプログラムである場合を示している。この場合、課金対象のコンテンツ情報の少なくとも一部は、コンテンツキーKcにより暗号化されており、当該コンテンツキーKcがライセンス情報に含まれている。

【0336】図96において、図92と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図96において、図92のデコーダ3053、D/A変換部3054がプログラム実行部3055に置き換わり、プログラム実行部3055にてコンテンツ情報としてのプログラムが実行されるようになっている。情報再生部3004にコンテンツキーKcと暗号化されたコンテンツ情報とが送られてくるまでの動作は、前述同様である。

【0337】この場合の情報再生部3004は、CPU、メモリ等から構成される中央処理装置であっても良い。

#### (1-10)

上記(1-1)～(1-9)は、図77に示したように、情報再生装置が時計3005を具備している場合である。勿論、復号判定カード3001自身が時計を内蔵する場合も考えられる。この場合、復号判定カード3001は時計の駆動用に電池を内蔵することになる。時計を復号判定カードに内蔵することのメリットは、図79に示した時刻転送部3012と、時計との間の認証処理が不要になることである。

(2) 以下、図76の情報流通システムについて説明する。

【0338】この場合の情報再生装置の構成および処理動作は前述の図75の場合とほぼ同様である。

【0339】図76の情報流通システムでは、リムーバブル情報蓄積メディアには、当初ライセンス情報は記録されておらず、コンテンツIDと暗号化されたコンテンツ情報とが記録されている。ライセンスの更新の際には、メディアと復号判定カードとをライセンス更新端末にセットする。更新端末はメディアからコンテンツID、復号判定カードから前述の公開マスターキーのうちの1つをそれぞれ読み取り、ライセンスサーバーに転送する。ライセンスサーバーは、取り扱いコンテンツのデータベースを具備しており、コンテンツIDをキーとしてデータベースを検索し、コンテンツキーを取得する。

【0340】ライセンスサーバーは次いで、コンテンツ

キーを含む通常のライセンス情報を作成し、公開マスターキーによって暗号化して、更新端末に転送する。更新端末は、受け取った暗号化ライセンス情報をメディアに記録する。ライセンス情報記録後のメディアの再生は、図75の情報流通システムの場合と同様である。

【0341】次に、図76の情報流通システムにおける、ライセンス更新端末とライセンスサーバーについてより詳細に説明する。

#### (2-1) ライセンス更新端末

ライセンス更新端末の構成を図97に示す。

【0342】ライセンス更新端末4000は、挿入された復号判定カードから所定の情報を読み取るカードインターフェース(IF)4001、挿入されたリムーバブル情報蓄積メディアから所定の情報を読み取るリムーバブル情報蓄積メディアドライブ4002、所定の通信回線(例えば公衆回線、専用回線等)を介してライセンスサーバとの間の通信を行うための通信部4003、例えば液晶表示パネル等から構成される表示部4004、ユーザからの指示を入力するためのキーボード、タッチパネル等から構成されるキー入力部4005から構成されている。

【0343】図98は、図97に示したライセンス更新装置4000の処理動作を示したフローチャートである。以下、図98を参照してライセンス更新端末の処理動作について説明する。

【0344】リムーバブル情報蓄積メディアドライブ4002にリムーバブル情報蓄積メディアがセットされると当該メディアからそのメディアに記録されているコンテンツ情報の識別情報、すなわちコンテンツIDが読み取られ(ステップS4001)、この読み取られたコンテンツIDと当該ライセンス更新端末の識別情報(更新端末ID)とが通信部4003を介してライセンスサーバに送信される(ステップS4002)。

【0345】ライセンス更新端末からライセンスサーバーに対して送信される更新端末IDは、ライセンスサーバーが更新端末IDを更新情報と共に、更新ログとして保存する際に用いられる。また、コンテンツ利用料金の回収は、この更新ログに基づいて行われてもよい。

【0346】コンテンツIDと更新と更新端末IDとを受信したライセンスサーバでは、当該更新端末に課金メニュー、要求キー種別情報、認証キー番号Nを送信する(ステップS4003)。

【0347】ライセンスサーバから更新端末に送られてくる要求キー種別情報は、前述の3種類のマスターキーの指定するためのものである。前述したように、要求キー種別は、例えば次のようなものがある。

- ・ 要求キー種別情報が「0」のとき…予め定められた復号用のマスターキー、すなわちKm(0)、…、Km(999)を指定

- ・ 要求キーの種別情報が「1」のとき…ライセンス情

報復号用の各判定カードでユニークなマスターキー、すなわちKP(1000)、…、KP(1499)を指定  
・ 要求キーの種別情報が「2」のとき…各判定カードで所定時間毎に更新される秘密鍵、KP(1500)、…、KP(1599)を指定

ライセンスサーバからライセンス更新端末に送られてくる認証キー番号Nは、復号判定カードが転送の際の認証用に保持しているキーKNを指定する番号である。このキーKNによって暗号化されたマスターキーKPは、ライセンスサーバが保持するKNに対応する復号鍵K'Nによって復号される。ライセンスサーバは、この様にして得たキーKPを用いてライセンス情報を暗号化して、ライセンス更新端末に送信する。従って、(例えば、正当でない装置が復号判定カードに成りすまそうとした場合の様に)復号判定カードが正しい認証キーKNを保持していない場合、リムーバブル情報記録メディアに記録されるライセンス情報は、KPに対応する復号鍵Ksによって復号することができない。かくして、正当でない復号判定カードは排除される。

【0348】課金メニューは、コンテンツ情報の有効期間に応じた料金表で、この課金メニューから所望の有効期間を選択して料金の支払を行うようになっている。課金メニューは例えば、有効期間に対応する料金と、その有効期間を選択する際の識別番号とから構成されている。具体的には、有効期間が7日間のときの料金は200円で識別番号は「1」、有効期間が30日間のときの料金は500円で識別番号は「2」、有効期限が無期限(譲渡)のとき料金は3000円で識別番号「3」となる。

【0349】なお、要求キー種別情報が「0」のとき、ライセンス更新端末はマスターキーKPをライセンスサーバに送る必要はない。何故なら、ライセンス情報が全ての復号判定カードに共通するキーで暗号化されて、ライセンスサーバから送られて来るからである。この場合、サーバから送られるライセンス情報にはKmの番号の指定が添えられている。この番号は暗号化されている必要はない。

【0350】更新端末とライセンスサーバとの間の通信回線が専用回線でない場合、情報セキュリティ対策として、ライセンスサーバの通信部4021と更新端末の通信部4003とが通信を行う際に相互認証の手続きを行うことが望ましい。この場合、ライセンス更新に対する課金はライセンス更新端末を設置する店舗で行う。正当でないライセンス更新端末を排除しなければ、課金が正しく行われない可能性があるからである。また、ライセンス更新端末の設置者にとっても正当でないライセンスサーバに接続すると、不正なライセンス情報で利用者に課金してしまう危険が存在するからである。

【0351】通信回線が専用回線で、通信先が信頼できる場合、相互認証は不要となる。なお、ライセンス更新

端末からライセンスサーバへの接続にインターネットなどの一般回線が利用されるライセンス更新端末の通信部4003は、ライセンスサーバとの通新記録を保存する様にしても良い。料金の回収はライセンスサーバの記録に基づいて行われるから、ライセンス更新端末側にも確認の為に記録を残しておく方が運用上好ましい。

【0352】さて、ライセンス更新端末の通信部は4003、ライセンスサーバから送信された情報のうち、課金メニューを表示部4004で転送し、要求キー識別情報と認証キー番号NとをカードIF4001に転送する(ステップS4004)。

【0353】表示部4004は課金メニューを提示して、ユーザに有効期間の識別番号の選択を促す。一方、カードIF4001は、要求キー識別情報と認証キー番号とを復号判定カードへ転送する。復号判定カードでは、これらの情報を受けて、要求キー識別情報に対応したマスターキーKP(複数のKPのうちの適当な1つ)を認証キー番号にて指定された認証キーKNで暗号化したもの、すなわち[KP]KNをカードIF4001へ転送する。その際、マスターキーの識別情報も転送するようにしてもよい。

【0354】通信部4003には、カードIFから転送された[KP]KNと、表示部4004を介してユーザにより指定された課金メニュー中の有効期間の識別番号とをライセンスサーバに送信する(ステップS4005へステップS4007)。

【0355】これを受けてライセンスサーバからは、少なくとも、当該更新端末から通知されたマスターキーKPにて暗号化されたライセンス情報、すなわち[ライセンス情報]KPが送信されて、更新端末の通信部4003が受信する(ステップS4008)。

【0356】[ライセンス情報]KPは、リムーバブル情報蓄積メディアドライブ4002にてそこにセットされているメディアに記録される(ステップS4009)。なお、メディアにはライセンスサーバから送信された[ライセンス情報]KPとマスターキーの識別情報とが記録されてもよい。

(2-2) 復号判定カード

図99は、復号判定カードの3015のライセンス更新装置とのインターフェースを司る復号判定カード3015の要部、すなわち、更新インターフェース(IF)3015の構成例を示したものである。

【0357】以下、図100に示すフローチャートを参照して図99の各構成部の処理動作について説明する。

【0358】図98のステップS4004で更新端末のカードIF4001から復号判定カード3015に対し転送された要求キー識別情報と認証キー番号Nとは入出力部4011に入力する(ステップS4011)。

【0359】入出力部4011は、要求キー識別情報をマスターキー選択部3061へ転送し、認証キー番号N

を認証キー選択部4014へ転送する(ステップS4012)。

【0360】マスターキー選択部3061は、マスターキー格納部3062を検索して、要求キー識別情報に適合するマスターキーKPを選択し、暗号部4012へ転送する(ステップS4013)。

【0361】認証キー選択部4014は、認証キー格納部4013を検索して認証キー番号Nの認証キーKNを選択し、暗号部4012へ転送する(ステップS4014)。

【0362】暗号化部4012は、マスターキーKPを認証キーKNで暗号化し、[KP]KNを生成する(ステップS4015)。  
[KP]KNは入出力部4011を介してライセンス更新装置へ出力される(ステップS4016)。

(2-3) ライセンスサーバ

図101は、ライセンスサーバの構成例を示したものである。

【0363】コンテンツ情報データベース(DB)4024には、例えば、コンテンツIDに対応させて次の様な情報が格納されている。

【0364】・コンテンツキー

・課金メニュー

・要求キー種別

以下、図101のライセンスサーバ4001の各構成部の処理動作について図102に示すフローチャートを参照して説明する。

【0365】図98のステップS4002でライセンス更新端末から送信されたコンテンツIDと更新端末IDは、通信部4021にて受信され、応答部4022へ転送される(ステップS4021)。

【0366】応答部4022はコンテンツIDをコンテンツ情報検索部4023へ転送し(ステップS4022)、コンテンツ情報検索部4023は、コンテンツIDを基にそれに対応するコンテンツキー、課金メニュー、要求キー種別を読み出し、これらの情報を応答部4022へ転送する(ステップS4023)。

【0367】一方、応答部4022は、認証キー番号Nを生成する(ステップS4024)。例えば、予め定められた複数の認証キー番号のうちから1つを選択するようにしてもよい。そして、コンテンツキー以外の情報、すなわち、課金メニュー、要求キー種別情報、認証キー番号Nを通信部4021を介してライセンス更新端末に送信する(ステップS4025)。

【0368】図98のステップS4007で更新端末から送信された[KP]KN、課金メニュー中の所望の有効期間の識別番号は、通信部4021で受信され、これらは応答部4022へ転送される(ステップS4026)。

【0369】応答部4022では、先に生成された認証

キー番号Nに対応する復号鍵KN'で[KP]KNを復号し、マスターキーKPを得る(ステップS4027)。

【0370】応答部4022にて生成されたライセンス情報は、暗号化部4025でマスターキーKPを用いて暗号化され([ライセンス情報]KPを生成し)、[ライセンス情報]KPは通信部4021を介してライセンス更新装置に送信される(ステップS4028～ステップS4029)。

【0371】応答部4022は、更新記録データベース(DB)4026に、ステップS4021にて受信した更新端末IDに対応させて、ライセンスの更新履歴情報を記録する(ステップS4030)。

(3) ユーザ端末から電子決済を利用してライセンス更新を行う場合の情報流通システム

図103に電子決済を利用してライセンスを更新する場合のユーザ端末、ライセンスサーバ4101、電子決済装置4102からなるシステム構成の一例を示したもので、ユーザ端末がネットワーク経由の電子決済によって、課金処理を行うようになっている。

【0372】ユーザ端末は、少なくともライセンス更新装置4103を具備するとともに、復号判定カード3001とリムーバブル情報記憶メディア4031とが装着された、例えばパーソナルコンピュータで構成されるものであってもよい。

【0373】図104は、ユーザ端末に具備されたライセンス更新装置4103の構成例を示したもので、CPU等から構成される制御部4044が通信部4041、リムーバブル情報記録メディアIF4042、復号判定カードIF4043、表示部4045、入力部4046の各構成部を制御して、ライセンスを更新するための処理を実行するようになっている。

【0374】図105はライセンスサーバ4101の構成例を示したもので、制御部4053が通信部4051、復号部4052、課金整理番号発行部4054、課金処理部4055、ライセンス情報生成部4056の各構成部を制御してライセンスを更新するための処理を実行するようになっている。

【0375】図106は、全てのライセンス判定カードに共通の(従って、全てのユーザ端末に共通の)マスターキー(例えばKm(0)、…、Km(999)のうちの1つ)によってライセンス情報が暗号化されている場合を例にとり、図103に示したシステム全体の処理動作を示したフローチャートである。

【0376】以下、図106に示したフローチャートを参照して、ライセンス更新装置4103、ライセンスサーバ4101の各構成部の処理動作を説明する。

【0377】なお、メディア4031にはコンテンツ情報とライセンス情報とが記録されており、ライセンス情報には、例えば該コンテンツ情報の利用の可否を判定す

るための利用条件やコンテンツID、その他の情報が含まれているものとする。

【0378】ライセンス更新装置4103のリムーバブル情報記録メディアインターフェース(IF)4042は、ユーザ端末にセットされたメディアからライセンス情報を読み取り、それを復号判定カードインターフェース(IF)4043を介して復号判定カード3001へ出力する(ステップS4041)。

【0379】復号判定カード3001では、例えば、入力されたライセンス情報に基づき所定の処理(例えば、第2の実施形態で説明した復号ユニットA等の処理動作参照)を行い、その結果、ライセンスの更新を行う場合、ライセンスの更新情報(例えば、復号ユニットAの場合、図56に示したような更新情報)を出力する。

【0380】復号判定カードIF4043は、次に、復号判定カード3001からライセンスサーバIDを読み取る(ステップS4042)。なお、ライセンスサーバIDは更新情報に含まれていてもよい。

【0381】ライセンスサーバIDは、ライセンスサーバを特定するための識別情報である。

【0382】ライセンス更新装置4103は、通信部4041を介してライセンスサーバIDにて特定されるライセンスサーバにアクセスしてライセンス情報を更新するための更新情報を送信する(ステップS4043)。

【0383】ライセンスサーバ4101の通信部4051が、ライセンス更新装置4103から送信された更新情報を受信すると、更新情報に含まれるコンテンツIDを基に課金データベース(DB)4058を検索して、少なくとも課金メニューを読み出し(必要に応じて要求キー種別情報、認証キー番号N等)、さらに、課金整理番号発行部4054で課金整理番号を発行し、少なくとも課金メニューと課金整理番号(以下、データ群Aと呼ぶことがある)を通信部4051を介してライセンス更新装置4103に送信する(ステップS4044)。

【0384】ライセンスサーバから発行される課金整理番号は、ライセンスサーバがトランザクション毎に適当に割り付ける番号である。課金整理番号は、後述する様に、課金確認の為に用いられる。

【0385】ライセンスサーバは通常、複数のユーザ、すなわちライセンス更新装置からのライセンス更新要求を処理する。従って、回線接続時間は可能な限り短くする事が好ましい。その為、ライセンス更新装置は、ライセンスサーバとの回線を適宜切断する。例えば、ライセンス更新装置の通信部4041には、ライセンスサーバからの応答待ち時間Twが予め定められていて、この時間内にライセンスサーバから応答がない場合は、回線を切断するようにしてもよい。また、複数nライセンス更新装置のそれぞれからのライセンス更新要求を区別する為に、ライセンスサーバは課金整理番号に基づいて、ライセンス情報の管理を行う必要がある。データ群Aを受

信したライセンス更新装置4103は、課金メニューを表示部4045に提示し(ステップS4045)、ユーザにより所望の有効期間の識別番号が選択されたら(ステップS4046)、ライセンス更新装置4103の通信部4041は電子決済装置4102にアクセスし、少なくとも課金整理番号とライセンスサーバIDと選択された有効期間の識別番号とそれに対応する料金の支払要求を行う(ステップS4047)。

【0386】電子決済装置4102は、ユーザからの要求に応じて所定の支払処理を行い、処理が成功すればライセンスサーバIDにて指定されるライセンスサーバ4101に、例えば有効期間の識別番号と決済金額と課金整理番号を支払証明として送信して支払処理の成功を通知する。また、支払要求元のライセンス更新装置4103へも例えば有効期間の識別番号と決済金額と課金整理番号とを支払証明として送信する(ステップS4048～ステップS4050)。ライセンス更新装置4103では、決済金額と課金整理番号を受信すると、ライセンスサーバIDにて特定されるライセンスサーバにアクセスして、少なくとも、ステップS4046で選択された有効期間の識別番号と上記決済金額と課金整理番号とを支払証明として送信する(ステップS4051)。

【0387】ライセンスサーバ4101の通信部4051にて受信された、電子決済装置4102から送信された支払証明と、ステップS4051にてライセンス更新装置4103から送信された支払証明とは、その課金整理番号に対応させて課金処理データベース(DB)4057に記録される。

【0388】課金処理DB4057には、例えば、次のような情報が各課金整理番号に対応させて記憶されている。

【0389】・ライセンス更新端末のID

・コンテンツキー

・電子決済装置からの支払証明(有効期間の識別番号、決済金額、課金整理番号)

・ライセンス更新装置からの支払証明(有効期間の識別番号、決済金額、課金整理番号)

ライセンスサーバ4101では、電子決済装置4102、ライセンス更新装置4103とからそれぞれ支払証明を受信すると、課金処理DB4057に記録し、課金処理部4055にて双方の支払証明にある決済金額と識別番号とが一致するか否かを確認する(ステップS4052)。一致していた場合に限り適正な支払が行われたと判断できる。このような支払証明の確認処理と並行して、ライセンスサーバ4101のライセンス情報生成部4056では、ステップS4043にてライセンス更新装置4103から送信されたライセンスの更新情報と、コンテンツ情報DB4024から検索されたコンテンツIDに対応するコンテンツキーとに基づき、少なくともライセンス情報中の利用条件、コンテンツキー等を変更

する（ライセンス情報を更新する）。

【0390】ライセンス情報には、例えば、次の様な情報が含まれている。

- ・コンテンツID
- ・暗号化されたコンテンツ情報を復号するコンテンツキー
- ・少なくとも有効期限を含むコンテンツ情報の利用条件
- ・ライセンス情報の作成時刻
- ・更新サーバID
- ・課金整理番号

ここで、更新サーバIDは、今回ライセンスの更新を行ったライセンスサーバを特定する識別情報である。更新サーバIDによって、必要に応じて、ライセンス情報から更新を行ったサーバを特定する事が可能となる。

【0391】ステップS4053で、適正な支払が行われたことが確認されると、ライセンスサーバ4101は、通信部4051を介して更新されたライセンス情報をライセンス更新元のライセンス更新装置4103に送信する（ステップS4054）。

【0392】更新されたライセンス情報を受信したライセンス更新装置4103では、リムーバブル情報記録メディアIF4042を介してメディア4031に該更新されたライセンス情報を記録する（ステップS4055）。

【0393】（第4の実施形態）図107は、第4の実施形態に係る情報再生システムの全体の構成例を示したもので、例えば、図53、図75、図76、後述する図122に示したような情報流通システムでユーザにより用いられるものである。コンテンツ情報は、DVD-RAM、DVD-ROM等の記録媒体（情報メディア）に記録されている。予め定められた条件下における当該コンテンツ情報の利用（再生および視聴）権をライセンスといい、このライセンスを購入することにより、ユーザにライセンス情報が与えられる。当該コンテンツ情報の再生を可能にするライセンス情報は、コンテンツ情報の記録されている記録媒体と一緒に記録されていてもよいし、コンテンツ情報とは別個に、その他の記録媒体あるいはメモリおよび演算機能を有するICカード等に記録されていて、コンテンツ情報とは別個に読み取られ、図107に示す情報再生装置に入力されるものであってもよい。あるいは、放送やインターネット等を通じて配信されるものであってもよい。

【0394】図107において、情報再生システムは、主にデジタルコンテンツである暗号化コンテンツ情報をDVD-ROM、DVD-RAM等の情報メディアから読み取る情報メディアドライバ7001、暗号化コンテンツに対応するライセンス情報に基づいて当該ライセンスが有効かどうかのチェックを行い、有効ならば当該コンテンツ情報を利用するためのコンテンツ復号鍵を出力する情報再生装置700、情報再生装置7000から出

力される復号鍵で暗号化コンテンツを復号し、再生する、DVDプレーヤ、ビデオ再生装置などの情報利用装置7002から構成される。

【0395】ライセンス料の着実な徴収のためデジタルコンテンツは予め暗号化されていると仮定している。本実施形態で用いるコンテンツ情報の構成例を図113に示す。即ち、コンテンツは暗号化部分と未暗号化部分に分かれ、暗号化部分には暗号化コンテンツが、未暗号化部分にはコンテンツIDが記録される。コンテンツIDはコンテンツとそのライセンス情報のリンクを取るためのものである。

【0396】図114は、ライセンス情報の構成例を示したもので、暗号化コンテンツを解除する復号鍵（以下コンテンツ復号鍵という）と、利用期限などのライセンス利用条件と、当該コンテンツのIDと、ライセンス認証情報とが含まれている。ライセンス認証情報とは、暗号化されたライセンス情報が正確に復号されたか否かをチェックするための定められたコードである。例えば、4バイトコードであれば16進数で「a5fe478e160e325f」と表されるようなコードである。これは、予めライセンス生成装置、ライセンス更新装置及びライセンス判定ユニットの間で定めておくべき情報である。

【0397】ライセンス情報は、その全体を予め定められた公開鍵で暗号化されている。このライセンス情報の復号は、情報再生装置7000に具備されるライセンス判定ユニット7008内で当該ユニット内に存在する秘密鍵を用いて行い、復号されたライセンス情報に基づいて利用条件のチェックを行う。利用条件として、例えば利用期限と利用回数とがある。利用条件として利用期限を採用することにより、利用期限後には視聴できなくなり、また、コンテンツと、そのコンテンツを復号するために必要なライセンス情報とをまるごと不正コピーしたとしても利用期限後には使えなくなるので海賊版の流通を実質的に意味のないものとすることができる。

【0398】だが、利用期限を定めた場合、その利用条件のチェックのための現在時刻（以下、時刻とは日付および時刻を意味するものとする）を計時する時計の管理を着実に行わないと、利用期限自体無意味なものとなる。例えば、12月15日に1週間分のライセンスとして12月22日までの利用期限を有するライセンス情報を取得したとしても、ライセンス判定ユニット7008が参照する時計が6月10日を示していたら半年分のライセンスになってしまうのである。特に、このようなことは時計が、ユーザに調整可能であれば、ユーザによって時計を都合良く調整される可能性があるので十分起こり得ることである。

【0399】そこで、本実施形態では、この点を改善し、時計を都合良く調整した場合でも利用期限を遵守させる枠組を提供できる情報再生装置について説明する。

すなわち、ライセンス情報の復号鍵を一定時間毎に予め定められたアルゴリズムで生成し、それ以前の復号鍵と置き換え、ライセンス生成装置やライセンス更新装置においても同じタイミングで対応するライセンス情報の暗号鍵を生成することによって、時計の時刻がライセンス生成装置もしくはライセンス更新装置のそれから著しくずれている場合は、新たに取得したライセンス情報が復号できなくなる。従って、少なくとも新しいコンテンツを視聴したい場合は時計の時刻を正確に合わせる必要があるのである。このようにライセンス情報の復号鍵を変化させることによって間接的に時計を正しい状態にするというのが本実施形態の主旨である。なお、図107において、現在時刻を計時するための時計7008h(図108参照)は、ライセンス判定ユニット7008の内部に設けられているが(この場合、ライセンス判定ユニット7008を例えば1つのICチップで構成し、ユーザにより計時時刻が調整されることがないようにハードウェア的に保護する構成が容易に行えるが)、時計7008hの計時時刻はユーザにより調整可能であってもよい。

【0400】次に、図109～図110に示すフローチャートを参照して、図107の情報再生装置の処理動作および図108に示すような構成のライセンス判定ユニット7008の処理動作について説明する。

【0401】情報メディアドライバ7001から読み取られた図113のようなコンテンツ情報は、データ分離部7007でコンテンツIDと暗号化コンテンツに分離される(ステップS7001～ステップS7002)。暗号化コンテンツは情報利用装置7002に送られ(ステップS7003)、ライセンス判定ユニット7008から出力されるコンテンツ復号鍵を待つ。

【0402】一方、コンテンツIDはライセンス情報検索部7006に送られる。ライセンス情報検索部7006は、ライセンス情報データベース(DB)7004から当該コンテンツIDを持ったライセンス情報を検索する(ステップS7004)。ライセンス情報DB7004に記憶されているライセンス情報は、図115に示すように、少なくともコンテンツIDを含む暗号化部を暗号化ライセンス情報に付加されていて、コンテンツIDで該コンテンツに対応するライセンス情報が検索できるようになっている。検索されたライセンス情報はライセンス判定ユニット7008へ送られる(ステップS7005～ステップS7006)。

【0403】図108は、ライセンス判定ユニット7008の構成例を示したものである。ライセンス情報検索部7006で検索されたライセンス情報は、ライセンス情報入力部7008aに入力し、復号部7008bへ転送される。

【0404】復号部7008bでは、復号鍵格納部7008eに格納されているライセンス情報復号鍵を使って

ライセンス情報を復号する(ステップS7007～ステップS7008)。

【0405】復号されたライセンス情報はライセンス情報整合性確認部7008cでライセンス認証情報を使ってライセンス情報が正しく復号されたことを確認する(ステップS7009)。すなわち、ライセンス情報が復号された際、ライセンス情報のデータ中の予め定められた場所にライセンス認証情報があるかどうかをチェックして、もしあればライセンス情報を正しく復号できたと判定する。もちろん適切な復号鍵で復号していれば通常このコードはでたためなものになる。もし、ライセンス情報が正しく復号されていないと判定した場合、ライセンス情報検索部7006へライセンス情報の次候補の検索を要請する。ライセンス情報検索部7008ではこれを受けてライセンス情報DB7004を検索し、当該コンテンツIDを持つ次のライセンス情報を抽出して、ライセンス判定ユニット7008に送る。もし、ライセンス情報検索部7006でライセンス情報の次候補が検索できなかった場合、図110のステップS7021へ進み、表示部7011に、例えば「ライセンス情報が無効であるか、参照時計の時刻が間違っています。現在の参照時計の時刻はYYYY年HH時MM分です。時刻を確認した上で、ライセンスの更新を行ってください。」という旨のメッセージの表示を要請する(図110のステップS7021)。これを見てユーザは現在の時刻を確認し、時刻が著しくずれていた場合は修正する。

【0406】復号鍵生成部7008fは、ライセンスを発行するライセンス更新装置、ライセンス作成装置とともに一定時間毎に鍵を新たに生成し、復号鍵格納部7008eに格納する。そのため、ライセンス判定ユニット7008の時計7008hが実際の時刻と著しくずれている場合、ライセンス判定ユニット7008で生成される復号鍵とライセンス更新装置もしくはライセンス生成装置で生成される暗号鍵との整合がとれず、従って、利用条件が有効なライセンス情報であっても復号できない。このため、上記表示メッセージのように、ユーザに時計7008hの時刻確認を求める必要がある。その後、ユーザの要求に応じてライセンスの更新を行うようにしてもよい。

【0407】さて、図109のステップS7010で、ライセンス情報整合性確認部7008cでライセンス情報が正しく復号されたと判定された場合、ライセンス情報は利用条件判定部7008dへ送られ、引続き利用条件の判定が行われる。利用条件として利用期限を用いているので、利用条件の判定は時計参照部7008gを介して、ライセンス判定ユニット7008の内部、場合によっては外部にある時計7008hの時刻を参照して、該時刻が利用期限内であるか否かを判定する(ステップS7011)。利用条件を満たしていると判定されれば(ステップS7012)、コンテンツ復号鍵が情報利用

装置7002に出力され(ステップS7013)、情報利用装置7002では、これを使って別途送られた暗号化コンテンツを復号し、再生利用する(ステップS7014)。

【0408】一方、ステップS7012でライセンスの利用条件が満たされていない場合は、その旨と少なくとも当該ライセンス情報とをライセンス情報検索部7006へ転送し、図110のステップS7021へ進み、ユーザからの要求に応じて、当該ライセンスの更新を行うようにしてもよい。

【0409】ライセンスの更新は、後に詳しく述べるような手続きで、図107のライセンス更新指示部7005、希望利用条件入力部7010、表示部7011などを通じて、図116に示したような、少なくともコンテンツIDと希望利用条件を含むライセンス更新情報を作成し、作成されたライセンス更新情報を例えばインターネットのような所定のネットワークを介してライセンス更新装置に送り、ライセンス情報の更新を行なう。

【0410】図110に示すフローチャートは、ライセンス情報の更新処理動作を示したもので、ライセンス情報検索部7006では、表示部7011に「ライセンス情報が無効であるか、参照時計の時刻が間違っています。現在の参照時計の時刻はYYYY年HH時MM分です。時刻を確認した上で、ライセンスの更新を行ってください。」という主旨のメッセージを表示した後(ステップS7021)、少なくともユーザがライセンス更新をするか否かの指示入力を行うための適切なインターフェースを具備したライセンス更新指示部7005を起動する。ユーザは、(例えば、時計7008hの時刻の確認等を行った後)、このインターフェースを介してライセンス更新を行う旨の指示入力を行ったとする。ライセンス更新指示部7005は、それをライセンス情報検索部7006に送り、ライセンス情報検索部7006は当該コンテンツIDをライセンス更新部7009に送る(ステップS7022～7024)。

【0411】ライセンス更新部7009は、希望利用条件入力部7010を起動し、希望利用条件入力部7010の適切なインターフェースを介して入力された希望利用条件と、ライセンス情報検索部7006から送られてきたコンテンツIDとを用いて、図116に示したようなライセンス更新情報を作成し(ステップS7025～ステップS7027)、当該ライセンス更新情報を所定のネットワークを介してライセンス情報更新装置に送る。

【0412】ステップS7024で、ユーザがライセンス更新をしない場合(すなわち、ユーザがライセンス更新指示部7005を介してライセンスを更新しない旨の指示入力を行った場合)、ライセンス情報検索部7006では、コンテンツIDを消去し、処理が終了する。

【0413】更新されたライセンス情報は、図111に

示すように、ICカード等を介して、あるいは、インターネット等の所定のネットワークを介してライセンス格納部7003に入力され、図115に示したようなデータ形式に変換されて、ライセンス情報DB7004に記憶される。

【0414】なお、ライセンス判定ユニット7008でライセンスが無効と判定された場合(図109のステップS7005、ステップS7010、ステップS7012)には、そのまま処理を中断(再生を中止)するようにしてもよい。この場合は、ライセンス更新指示部7005、表示部7011、ライセンス更新部7009、希望条件入力部7010は不要となり、ライセンス更新装置と通信を行う機能も不要となり、構成も簡略となる。ライセンスを更新する際は、ユーザが例えばICカードをもってライセンス更新を行う代理店等に赴き、所定の料金を支払い、利用条件等の更新された新たなライセンス情報を該ICカードへ書き込んでもらう。そして、該ICカードを持ち帰り、再び図107の情報再生装置へ挿入して、該更新されたライセンス情報を読み込ませて、ライセンス格納部7003を介してライセンス情報DB7004へ格納する。

【0415】次に、ライセンス情報の復号鍵の生成処理動作について、図112に示すフローチャートを参照して説明する。

【0416】ライセンス判定ユニット7008の復号鍵生成部7008fは、時計参照部7088gを介して時計7008hを参照し、予め定められた時刻になったら復号鍵の生成を開始し(ステップS7041～ステップS7042)、生成された復号鍵は、復号鍵格納部7008eに格納する(ステップS7043～ステップS7044)。復号鍵の生成はライセンス生成装置及びライセンス更新装置と同期して行わなくてはならないものであり、例えば一週間に1度、毎週月曜日の午後15:00というように決まった時間に更新する。また、その主旨からライセンス生成装置やライセンス更新装置と同じ鍵を作らなければならない。このため、例えば時刻をシードとした乱数生成器での鍵生成が考えられる。即ち、1997年12月15日に変更する場合は数字「19971215」をシードとして、例えば復号鍵生成部7008fに具備された乱数生成器の出力を復号鍵とするのである。勿論、ライセンス生成装置及びライセンス更新装置でも同じ方式でライセンス情報の暗号鍵生成する。

【0417】以上は、共通鍵方式の場合の共通鍵を作る方式であるが、ライセンス判定ユニット7008が公開鍵暗号を採用している場合もある。この場合は、前述の復号ユニットAの鍵生成部2006の場合の説明と同様に、例えばRSA暗号の鍵生成のアルゴリズムを用いて、復号鍵(秘密鍵)を生成すればよい。

【0418】以上によって一定時間毎にライセンス生成装置とライセンス更新装置及びライセンス判定ユニット

7008の双方で復号鍵が変更できる仕組みができる。このため、ライセンス判定ユニット7008を含む情報再生装置内の時計7008hをユーザの操作によって改変されても、新たに取得したライセンス情報は復号でなくなることから、時計の改変は多くの場合防止できる。

【0419】なお、このような特徴から、時計7008hがユーザの操作によって改変可能かどうかはあまり問題ではなくなる。

【0420】また、鍵生成のプロセスにおいても、鍵生成の開始指示をを復号鍵生成部7008f自身が出すのではなく、時計参照部7008gもしくは時計7008h自身が出すことも考えられる。この場合、復号鍵生成部7008fが主導して復号鍵を生成するよりも、より正確な時刻に鍵生成が行える。

【0421】さらに、本実施形態では、1つのコンテンツに対応したライセンスを検索したら、その有効判定（有効期限のチェック）を行ない、有効なら復号鍵を出力する。しかし、無効な場合、他のライセンス情報を検索せず、ライセンスが失効したか、参照時計が間違っている旨の表示を行うことになっている。これは当該コンテンツに対応したライセンス情報が1つのみと暗黙に仮定しているためである。しかし、例えば2週間分のライセンスを購入・販売する際、ライセンス情報を1週間毎に分離する場合もある。更に期間限定のライセンス以外に回数限定のライセンスを販売し、同じコンテンツに関してこれらが共存する場合もある。このような時は、存在するライセンス情報を全て検索し、ユーザにとって最も有利なライセンスを利用するように構成することも可能である。

【0422】例えば、期間限定ライセンスの方を回数制限ライセンスよりも優先することによって、期間限定のライセンスがあるうちは回数限定のライセンスを使わなくてもすむので、ユーザにとっては有利である。この場合、ライセンス情報DB7004に記憶されるライセンス情報は、図117に示すように、未暗号化部にはコンテンツIDの他に期間限定のライセンスかあるいは回数限定のライセンスかを識別するための情報が含まれていることが望ましい。

【0423】ライセンスを選択する際の優先順位は、ユーザ自身で指定できるようにしてもよい。例えば、ライセンス情報検索部7006が表示部7011に、期間限定のライセンスと回数限定のライセンスにいずれを優先するかをユーザに選択させるためのメニュー画面を表示してもよい。

【0424】また、ライセンス情報検索部7006は、最優先のライセンス情報が出現すればライセンス情報を全て検索しなくても、その時点で検索を終了するようにしてもよい。

【0425】図118は、図107に示した情報再生装

置7000の他の構成例を示したもので、コンテンツ情報は、DVD-RAM、DVD-ROM等の記録媒体（情報メディア）に記録され、ライセンス情報は、放送にて配信されるものとする。

【0426】図118の情報再生装置では、放送配信される暗号化ライセンス情報の復号鍵を放送波に含まれるシードを基に生成することを特徴とし、その結果、復号鍵の生成を前述の時計7008hを利用することなしに行うことができる。

【0427】なお、図118において、図107と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図118に示す構成では、暗号化ライセンス情報が放送波によって送られ、その放送波には暗号化ライセンス情報の復号鍵を生成するためのシード情報が混在しているため、当該放送波を受信し、デジタル信号に変換するためのライセンス情報受信部8001と、ここで受信された放送波から暗号化ライセンス情報とシード情報とを分離するためのライセンス分離部8002とを具備し、ライセンス判定ユニット8009では、放送波にて送られていたシード情報に基づき復号鍵を生成するようになっている。

【0428】図121は、ライセンス情報受信部8001で受信される放送波のデータ構造の一例を示したものである。ライセンス情報とシード情報のそれぞれの先頭には、ライセンス情報とシード情報とを識別するための固定長の識別情報が付加されている。

【0429】図119は、図118のライセンス判定ユニット8009の構成例を示したものである。なお、図119において、図108と同一部分には同一符号を付し、異なる部分についてのみ説明する。すなわち、図119に示すライセンス判定ユニット8009では、ライセンス分離部8002から出力されたシード情報が入力する復号鍵生成シード入力部8009gをさらに具備し、復号鍵生成部8009fでは、シード情報から復号鍵を生成するようになっている。

【0430】次に、図120に示すフローチャートを参照して、受信した放送波から、暗号化ライセンス情報と復号鍵のシード情報を分離して復号鍵を生成するまでの動作について説明する。

【0431】ライセンス情報受信部8001では、放送波を受信し、図121に示すように受信データを得ると、その受信データを一旦ライセンス分離部8002へ送り、識別情報を用いてライセンス情報とシード情報とに分解する（ステップS8001～ステップS8002）。

【0432】受信データがライセンス情報であった場合、それをライセンス格納部7003に送る（ステップS8003～ステップS8004）。ライセンス格納部7003では、ライセンス情報を図115に示したようにコンテンツIDを付加して、ライセンスDB7004



に格納する。一方、受信データがシード情報であった場合、当該シード情報をライセンス判定ユニットに送る（ステップS8005）。ライセンス判定ユニットでは、これを、復号鍵生成シード入力部8009gで受け、復号鍵生成部8009fに送り、新たな復号鍵を生成する（ステップS8006）。復号鍵生成部8009fでは、例えば、シード情報から第4の実施形態と同様、共通鍵方式、公開鍵方式のいずれをもちいてもよい。生成された復号鍵は復号鍵格納部8009eに格納される。

【0433】ライセンス判定やライセンス更新の処理動作は、図109～図110と同様である。

【0434】放送によってライセンス情報を配信する場合、ライセンスを全ての情報再生装置（受信端末）に送ったのでは、同じ仕様の受信端末を持った全ての人が視聴可能となってしまうので、ライセンスの管理をしているとは言えない。そのため、ライセンス情報を受信端末毎に与える必要があり、ライセンス情報の中に受信端末IDを入れ、当該IDを持つ受信端末以外の受信端末は受信できないようにする必要がある。そのため受信端末では、自分宛のライセンス情報のみを選別受信できるように、放送配信されるライセンス情報識別情報中に各受信端末を識別するための識別情報（受信端末ID）が含まれていることが望ましい。ここで、ライセンス情報識別情報中の受信端末IDを有効端末IDと呼ぶ。

【0435】各受信端末、すなわち、図118に示したような情報再生装置のライセンス分離部8002には、予め固有の受信端末IDが記録されている。そして、図121に示したような受信データからライセンス情報を分離する際に、ライセンス情報識別情報に含まれる有効端末IDと、自身のもつ受信端末IDとを比較し、一致したときのみ当該ライセンス情報を取り込むようにする。あるいは、一旦全てのライセンス情報を所定のメモリに記憶しておいてから、そのメモリに記憶されたライセンス情報識別情報中の有効端末IDと受信端末IDとを比較して、不要なライセンス情報を当該メモリから消去するようにしてもよい。

【0436】なお、図107、図118に示した情報再生装置7000は、汎用的なコンピュータに標準装備されているハードウェア資源を用いて構成することも可能である。

【0437】また、本実施形態で説明したライセンス情報の復号鍵生成処理動作は、第2の実施形態で説明した復号ユニットA、Cの鍵生成部2006においても適用できる。

【0438】さらに、ライセンス情報に本実施形態で説明したようなライセンス認証情報が含まれている場合、ライセンス情報整合性確認部7008cでライセンス認証情報を用いてライセンス情報が正しく復号されたか否かを確認する処理動作は、第2の実施形態で説明した復

号ユニットA～Dの判定部2003においても同様に行える。すなわち、復号ユニットA～Dの判定部2003では、ライセンス認証情報を照合することにより、当該ライセンス情報が正しく復号できたと判断された後に所定のライセンス判定を行えばよい。

【0439】以上説明したように、上記第4の実施形態によれば、ライセンス情報を復号するための鍵情報をライセンス判定ユニット7008内で予め定められた時間毎に生成することにより、コンテンツ情報の利用条件やコンテンツ情報の復号化鍵を含むライセンス情報の情報セキュリティの向上が図れる。

【0440】また、復号されたライセンス情報には、復号結果の正否を判定するためのライセンス認証情報が含まれていることにより、時間の経過に従って該ライセンス情報の復号化鍵がいくつも生成される状況であっても、そのうちのいずれか正しい復号鍵で当該ライセンス情報が復号されたか否かを容易に判断できる。

【0441】また、ライセンス情報の復号化鍵は、情報再生装置に放送配信されてくるシード情報に基づきライセンス判定ユニット8009内で生成されるので、当該復号鍵の更新が容易に行える。

（第5の実施形態）

（5-1）概略

図122は、第5の実施形態に係る情報流通システムの構成例を示したもので、課金対象である暗号化されたコンテンツ情報は、DVD等のリムーバブル情報蓄積メディア（以下、簡単にディスクと呼ぶ）Dに予め記録されており、ディスクDに記録されているコンテンツ情報を再生可能にするライセンスを購入してディスクDを貸し出すことによりなるレンタルサービスを提供するためのものである。ここで、ライセンスとは、予め定められた条件下におけるレンタルされるディスクDに記憶されているコンテンツ情報の利用（再生および視聴）権をいう。具体的には、例えば、限られた期間内、限られた回数だけ、コンテンツ情報を再生可能にするライセンス情報をユーザに売ること、当該ライセンスを与えることになる。

【0442】コンテンツ情報の再生を可能にするためのライセンス情報は、ICカード等の演算機能を有するカード型記録媒体（以下、簡単にカードと呼ぶ）Pに記録して各ユーザに渡される。

【0443】レンタル用のディスクDを提供する各店舗には、ライセンス注入装置5003が設置され、これらライセンス注入装置5003とセンターとが所定の通信回線を介して接続されてネットワークを形成している。図122に示したような情報流通システムのサービスに加入しているユーザが、このネットワーク上の任意の店舗に赴き、所望のコンテンツ情報の記録されたディスクDをレンタルするときは、まず、当該コンテンツ情報の視聴期間等のコンテンツ利用条件に対する料金の支払い

等の所定の手続きを行う。ライセンス注入装置5003は、センターから送られてきた当該ディスクDのディスクキーと利用条件等を含むディスク情報に基づきライセンス情報を作成して、カードPに記録する。

【0444】ユーザは、ディスクDおよびカードPを持ち帰り、カードPを当該情報流通システムに適合したカードアダプタ5004に挿入し、ディスクDをプレーヤー5005にセットすることにより、ライセンス情報に含まれる利用条件を満たす限り（例えば視聴期間内であれば）、当該コンテンツ情報の再生が可能となる。

【0445】図123は、店舗にあるレンタル用のディスクDに記録されているデータの一例を示したものである。図123に示すように、ディスクDには、ディスクID、1または複数の（例えば2種類の）暗号化コンテンツ情報、コンテンツ情報を復号するための各コンテンツ情報のそれぞれに対応する暗号化されたコンテンツキーとが記録されている。

【0446】1枚のディスクに記録されているコンテンツ情報は、そのそれぞれに対応するコンテンツキーにて暗号化されており、そのコンテンツキーは、当該ディスクのディスクIDに予め定められたディスクキーにて暗号化されている。ディスクキーは当該ディスクには記録されていないことが特徴である。

【0447】ディスクIDは各ディスクを識別するための識別情報で、各ディスク毎にユニークに定められていても良いし、同一タイトルのコンテンツ情報を記憶するディスクに共通であっても良い。あるいは、同じ製造工場で同じ日に製造されたディスクのディスクIDは共通であってもよい。

【0448】ディスクIDに対して、そのディスクに記録されている暗号化コンテンツキーを復号することのできるディスクキー（ディスク内には含まれていないが）は一意に定まる。が、逆は必ずしも真ではない。即ち、コンテンツキーを復号する為のディスクキーが同じであるからと言って、ディスクIDが同じであるとは限らない。

【0449】レンタル用のディスクDには、図123に示したようにディスクキーが含まれていない。ディスクDをレンタルするときは、そのディスクDに記憶されているコンテンツを復号するために必要なディスクキーをユーザに配信する必要がある。

【0450】そこで、ディスクDをレンタルする際には、センタに設けられたライセンス作成装置5001で当該ディスクDに対応するディスクキーを含むディスク情報を作成するようになっている。ディスクキーは、例えば図124に示したように、センタに設けられたコンテンツDB5002にディスクIDに対応させて予め記憶されている。

【0451】本発明は、ディスクキーの安全な配送方式を提供するものである。

【0452】図125に、図122に示した情報流通システムにおけるディスクキーの配送方式を概略的に示したものである。大きく分けて、ライセンス作成装置5001とライセンス注入装置5003とで鍵（ディスクキー）配信装置を構成し、カードアダプタ5004とプレーヤー5005とで鍵配信装置から配信された鍵（ディスクキー）を用いてコンテンツ情報を利用（例えば再生）する情報利用装置を構成する。ライセンスの有効性を判定するための判定装置はカードアダプタ3004が具備している。

【0453】ディスクキーが、ライセンス作成装置5001からカードアダプタ5004に送りとどけられるまで、ディスクID、コンテンツの利用条件とともに暗号化鍵 $k_e$ で暗号化されている。すなわち、ライセンス情報作成装置5001では、ディスクキーとディスクIDと利用条件とを含むディスク情報を作成し、さらに暗号化鍵 $k_e$ で暗号化してから配信し、復号化鍵 $k_d$ を予め保持しているカードアダプタ5004で復号することにより、途中の配信経路で盗聴等されてもディスクキーが解読される危険性を低くすることができる。

【0454】なお、鍵配信装置を構成するライセンス作成装置5001とライセンス注入装置5003とは、互いに利害関係を有する異なる者に別個に属する場合があります。その場合には、その利害関係を調整するために（ライセンス作成装置5001からライセンス注入装置5003へ配信する過程でディスク情報を不正に取得されることがないようにするため）、ライセンス作成装置5001では、ディスク情報を暗号化してからライセンス注入装置5003へ配信することが望ましい。

【0455】ディスクキーを含む暗号化されたディスク情報がカードアダプタ5004に到達するまでには、ライセンス注入装置5003、カードPとを経由する。そこで、この間における配信経路上でディスク情報を保護するため、暗号化されたディスク情報をさらに暗号化してライセンス注入装置5003からカードアダプタ5004まで配信する。

【0456】例えば、図125に示すように、ライセンス注入装置5003では、ライセンス作成装置5001から配信された暗号化鍵 $k_d$ で暗号化されたディスク情報に他の情報データを付加してライセンス情報を作成し、そのライセンス情報を共通鍵 $w_{12}$ で暗号化してカードPに書き込む。

【0457】共有鍵 $w_{12}$ は、例えば、DH鍵配送方式（Diffie-hellman Key Distribution Scheme）のように、カードPを介してカードアダプタ5004とライセンス注入装置5003との間で交換される公開してもかまわない情報（公開パラメータ）と、カードアダプタ5004とライセンス注入装置5003のそれぞれで保持される秘密パラメータとから生成される。公開パラメータはカードアダプ

タ5004とライセンス注入装置5003のそれぞれで保持される秘密パラメータから生成される。公開パラメータだけを知っている盗聴者は共有鍵w12は作れないようになっている。

【0458】共有鍵w12で暗号化されたディスク情報を復号できるのは、公開パラメータをライセンス注入装置5003と交換し合ったカードアダプタ5004だけである。

【0459】カードアダプタ5004は、カードPを介してライセンス注入装置5003から配信された公開パラメータと、自身で保持する秘密パラメータとから共有鍵w12を生成し、この共有鍵を用いて、同じくカードPを介してライセンス注入装置5003から配信された暗号化ライセンス情報を復号し、暗号化ディスク情報を得る。この暗号化ディスク情報を、復号化鍵keを用いて復号し、利用条件等をチェックして再生可否を判定する。再生可と判定したときは、ディスク情報に含まれるディスクキーをプレーヤ5005に渡す。

【0460】カードアダプタ5004とプレーヤ5005との間が盗聴されるかもしれない安全でない通信路であるならば、やはり、ディスクキーを暗号化してから配信することが望ましい。そこで、例えば、DH鍵配送方式のように、カードアダプタ5004とプレーヤ5005との間で交換される公開パラメータと、カードアダプタ5004とプレーヤ5004のそれぞれで保持される秘密パラメータとから生成される共有鍵wd2を用いて、カードアダプタ5004でディスクキーを暗号化してからプレーヤ5005へ配信する。

【0461】ライセンス作成装置5001でディスクキーを暗号化する際、ディスクID、コンテンツの利用条件等を付加してディスク情報を作成してから暗号化する。また、ライセンス注入装置5003でディスク情報を暗号化する際には、カードPの識別情報(KID)、カードアダプタ5004の識別情報(AID)等を付加してライセンス情報を付加してから暗号化する。ライセンス情報には、さらに、当該ライセンス情報の作成時刻が含まれていてもよい。

【0462】カードアダプタ5004およびカードPでは、それぞれの識別情報が外部から読取り、修正等が不可能なように保護されていることが望ましい。

【0463】ライセンス情報にカードPの識別情報(KID)、カードアダプタ5004の識別情報(AID)を含める場合、ライセンス注入装置5003は、ライセンス情報を作成する以前に、KID、AIDを取得する必要がある。

【0464】カードPから、その識別情報KIDをライセンス注入装置5003へ配信するときは、KIDを暗号化してから配信することが望ましい。そこで、例えば、DH鍵配送方式のように、ライセンス注入装置5003とカードPとの間で交換される公開パラメータと、

ライセンス注入装置5003とカードPとのそれぞれで保持される秘密パラメータとから生成される共有鍵wkを用いて、カードPで識別情報KIDを暗号化してからライセンス注入装置5003へ配信する。

【0465】カードアダプタ5004から、その識別情報AIDをライセンス注入装置5003へ(カードPを介して)配信するときは、AIDを暗号化してから配信することが望ましい。そこで、例えば、DH鍵配送方式のように、ライセンス注入装置5003とカードアダプタ5004との間で交換される公開パラメータと、ライセンス注入装置5003とカードアダプタ5004とのそれぞれで保持される秘密パラメータとから生成される共有鍵w11を用いて、カードアダプタ5004で識別情報AIDを暗号化してからライセンス注入装置5003へ配信する。ライセンス情報にカードPの識別情報(KID)、カードアダプタ5004の識別情報(AID)が含まれているとき、カードアダプタ5004では、ライセンス情報に基づき再生可否を判定する際、カードアダプタ5004自身のAIDと、現在カードアダプタ5004に挿入されているカードPのKIDと照合することができ、より情報セキュリティの向上が図れる。

【0466】図125に示すように、ディスクキーをライセンス作成装置5001からユーザ側の情報再生装置へ安全に配信するために、その配信経路上の各機器には、以下に示すような秘密パラメータを含む秘密情報を保持している。

【0467】・ライセンス作成装置5001は、ディスク情報を暗号化するための暗号化鍵Keを保持し、カードアダプタ5004はディスク情報を復号するための復号化鍵Kdを保持している。

【0468】・カードアダプタ5004とライセンス注入装置5003とは、両者が互いに認証し合い、ライセンス情報の暗号化復号化のために用いる、数X(1)と、同一のシードを与えた時同一の鍵を生成する鍵生成アルゴリズムA1(P1)と、十分大なる素数Pr1とを共有する。これらは、両者の認証と、ライセンス情報の暗号化復号化のために用いられる。ただし、P1はアルゴリズムA1のパラメータで、カードアダプタ5004とライセンス注入装置5003とは、アルゴリズムA1及びパラメータP1とを共有している。X(1)、A1、P1、Pr1は、カードアダプタ5004とライセンス注入装置5003とに外部からの読み取りが困難である様に保護されて記憶されている。

【0469】・ライセンス注入装置5003とカードPとは、数X(k)と、同一のシードを与えた時同一の鍵を生成する鍵生成アルゴリズムAk(Pk)と、十分大なる素数Prkとを共有する。これらは、両者の認証と、カードPの識別情報KIDの暗号化復号化のために用いられる。ただし、PkはアルゴリズムAkのパラメ

ータであり、ライセンス注入装置5003とカードPとは、アルゴリズムAk及びパラメータPkとを共有している。X(k)、Ak、Pk、Prkは、ライセンス注入装置5003とカードPとに外部からの読み取りが困難なように保護されて記憶されている。

【0470】・カードアダプタ5004とカードPとは、数X(k)と、同一のシードを与えた時同一の鍵を生成する鍵生成アルゴリズムAk(Pk)と、十分大なる素数Prkを共有する。これらは、両者の認証と、カードPの識別情報KIDの暗号化復号化のために用いられる。ただし、PkはアルゴリズムAkのパラメータであり、カードアダプタ5004とカードPとは、アルゴリズムAk及びパラメータPkとを共有している。X(k)、Ak、Pk、Prkは、ライセンス注入装置5003とカードPとに外部からの読み取りが困難である様に保護されて記憶されている。

【0471】・カードアダプタ5004とプレーヤー5005とは、数X(D)と、同一のシードを与えた時同一の鍵を生成する鍵生成アルゴリズムAD(PD)と、充分大なる素数PrDを共有する。これは、両者の認証と、ディスクキーの暗号化復号化のために用いられる。ただし、PDはアルゴリズムADのパラメータであり、カードアダプタ5004とプレーヤー5005とはアルゴリズムADとパラメータPDとを共有している。X(D)、AD、PD、PrDは、カードアダプタ5004とプレーヤー5005とに外部からの読み取りが困難である様に保護されて記憶されている。

【0472】・プレーヤー5005は復号化鍵KpD、カードPは復号化鍵KpC、カードアダプタ5004は復号化鍵KpA、ライセンス注入装置5003は復号化鍵KpLをそれぞれ外部からの読み取りが困難である様に保護されて記憶されている。復号化鍵KpD、KpC、KpA、KpLは、公開鍵暗号方式の公開鍵である。これらに対応する4つの秘密鍵KsD、KsA、KsC、KsLは、ライセンス作成装置5001が保持している。これら公開鍵および秘密鍵は、前述のX(1)、X(k)、X(D)、パラメータPl、Pk、PD、素数Pr1、Prk、PrD等を更新する際に利用される。

【0473】このように、ディスクキーは、暗号技術によって2重に保護されて配信されている。

【0474】(5-2) ライセンス作成装置

図126は、ライセンス作成装置5001の構成例を示したもので、以下、図131に示すフローチャートを参照しながら、ライセンス作成装置5001の構成およびディスク情報作成処理動作について説明する。

【0475】ディスク情報の作成は、例えば12時間毎に行われる。簡単な為、コンテンツの利用条件として、視聴可能期限(有効期限)を用い、コンテンツの視聴可能期間は1週間と予め定められたライセンスを与えるデ

ィスク情報を作成するものとする。

【0476】さて、視聴可能期間の開始時刻は0時及び12時であるとしよう。ライセンス作成装置5001は、例えば3時間前にディスク情報の作成を開始する。即ち、21時と9時にディスク情報の作成を開始する。視聴可能期間が9時から開始されるライセンスを与えるディスク情報の作成について述べる。9時に時計5001aから情報取得部5001bに対してディスク情報作成指示が発行される(ステップS5001～ステップS5002)。情報取得部5001bは有効期限作成部5001cに対して時計5001aから受け取った現在の日時情報(例えば、1981年4月2日9時)を送信する(ステップS5003)。

【0477】有効期限作成部5001cは、日時情報に基づき、その日の12時から起算して一週間後の有効期限の日時(例えば、1981年4月9日12時)を情報取得部5001bに返す(ステップS5004)。次いで、情報取得部5001bは、コンテンツDB5002から、ディスクIDとディスクキーの1対の情報を読み出し、それを有効期限とマージしてディスク情報を作成し、第1の暗号化部5001dへ転送する(ステップS5005)。ディスク情報には、ディスクID、ディスクキー、有効期限とが含まれている。

【0478】第1の暗号化部5001dは、第1の暗号鍵格納部5001eから暗号化鍵keを読み出し、ディスク情報を暗号化する(ステップS5006)。当該暗号化ディスク情報は平文のディスクIDが付加されて、所定のネットワークを経由してライセンス注入装置5003へ配信される(ステップS5007)。

【0479】以上ステップS5005～ステップS5007の処理を繰り返し、コンテンツDB5002に登録されている全てのコンテンツIDについてのディスク情報を作成する(ステップS5008)。

【0480】ライセンス注入装置5003は、ライセンス作成装置5001から受信した暗号化ディスク情報を、内部のライセンスDB5003f(図127参照)に、図132に示すように、ディスクIDに対応させて記憶する。

【0481】ディスク情報に有効期限が含まれていることは重要である。ライセンス注入装置5003は店舗に置かれ、攻撃の対象になりやすいとは言え、万一の盗難と言うことも考えられる。しかし、有効期限が含まれているディスク情報は、永久のライセンスを保証しないので、ライセンス注入装置5003を盗む動機は弱められる。のみならず、ディスク情報を解読して永久ライセンスの窃盗(即ち、ディスクキーの取得)を試みる為には、カードアダプタ5004に格納されている復号鍵Kd及びディスク情報の暗号化復号化用の秘密情報を盗む必要がある。ところが、復号鍵Kdも秘密情報もハードウェア的に厳重に保護されていれば、この作業は非常に

困難である。

【0482】(5-3)ライセンス注入装置

図127はライセンス注入装置5003の構成例を示したものである。

【0483】カードPは、カード装着部5003aに挿入される。カード装着確認部5003bにより、カードPが正常に装着されていることが確認されると、カードPとライセンス注入装置5003とは、カード装着部5003aを介して通信可能な状態となる。

【0484】乱数生成部5003kは、カードPのID(KID)、カードアダプタ5004のID(AID)、ライセンス情報(Lic)の暗号化・復号化に用いる乱数a1、c1、akを発生する。

【0485】ベース格納部5003mには秘密パラメータX(1)、Pr1、X(k)、Prkとが予め格納されている。

【0486】巾乗演算部5003jは、乱数生成部5003kで発生された乱数とベース格納部5003mに格納されている秘密パラメータとから公開パラメータ(第1～第3のシード生成情報)を計算する。また、カードPから転送されてくる第1のシード生成情報と乱数生成部5003kで発生された乱数akとから第1のシードを生成する。また、カードPを介してカードアダプタ5004から転送されてくる第2のシード生成情報と乱数生成部5003kで発生された乱数a1とから第2のシードを生成する。また、カードPを介してカードアダプタ5004から転送されてくる第2のシード生成情報と乱数生成部5003kで発生された乱数c1とから第3のシードを生成する。

【0487】例えば、乱数a1と秘密パラメータ(X(1)、Pr1)とから第2のシード生成情報 $X(1)^{a1} \pmod{Pr1}$ を計算する。以下、巾乗を表す場合、記号「 $\wedge$ 」を用いて、「 $X(1) \wedge a1$ 」と記す。また、modは剰余(この場合、 $X(1)^{a1}$ を素数Pr1で乗算したときの剰余)を表す。また、乱数akと秘密パラメータ(X(k)、Prk)とから第1のシード生成情報 $X(k) \wedge ak \pmod{Prk}$ を計算する。

【0488】共有鍵生成部5003lには、鍵生成アルゴリズムA1(P1)、Ak(Pk)が予め格納されている。第1のシードにアルゴリズムAk(Pk)を適用して第1の共有鍵wk1を生成し、第2のシードにアルゴリズムA1(P1)を適用して第2の共有鍵w11を生成し、第3のシードにアルゴリズムA1(P1)を適用して第3の共有鍵w12を生成する。第1～第3のシードに鍵生成アルゴリズムA1(P1)、Ak(Pk)を適用することにより、第1～第3のシードのデータ長を小さくすることができる。

【0489】復号部5003dは、共有鍵生成部5003lで生成された共有鍵wk1、w11、を用いて、暗

号化されたカードID([KID]wk1)、暗号化されたカードアダプタID([AID]w11)を復号する。

【0490】ディスク接続部5003gには、ユーザがレンタル使用とするディスクDが挿入されて、当該ディスクDのID(DID)を読み取る。

【0491】カードデータベース(DB)5003iは、ユーザに発行されるカードPのIDとそれに対応するカードアダプタ5004のIDとの対応関係を記憶するためのものである。

【0492】ライセンスデータベース(DB)5003fは、ライセンス作成装置5001から転送されてきた暗号化ディスク情報を記憶するためのもので、図132に示すように、暗号化ディスク情報は、ディスクID(DID)との対応させて記憶されている。

【0493】ライセンス作成部5003eは、ユーザがディスクをレンタルしようとする際に、そのディスクに対するライセンスを作成する。すなわち、ディスク接続部5003gで読み取られた当該ディスクDのID(DID)をキーとしてライセンスDB5003fから暗号化ディスク情報を検索し、カードDB5003iからユーザの所持するカードPと、カードアダプタ5004のID(KID、AID)を読み取り、さらに、時計5003hから現在時刻を読み取って、暗号化ディスク情報、ライセンス作成時刻、KID、AIDを含むライセンス情報を作成する。

【0494】なお、ここで作成されたライセンス情報は、カードPを介してカードアダプタ5004との間で交換された公開パラメータに基づき生成される共有鍵w12で暗号化される。

【0495】制御部5003cは、ライセンス注入装置5003全体の制御を司るものである。

【0496】(5-4)カード

図128は、カードPの構成例を示したものである。

【0497】カードPは、機器装着部5101を介して、ライセンス注入装置5003、カードアダプタ5004に接続し、機器装着確認部5102により、カードPがライセンス注入装置5003あるいはカードアダプタ5004に正常に装着されていることが確認されると、カードPとライセンス注入装置5003あるいはカードアダプタ5004とは、機器装着部5101を介して通信可能な状態となる。乱数生成部5107は、カードPのID(KID)をライセンス注入装置5003およびカードアダプタ5004へ転送する際に、カードID(KID)の暗号化・復号化に用いる乱数bk、dkを発生する。

【0498】ベース格納部5109には、秘密パラメータX(k)、Prkとが予め格納されている。

【0499】巾乗演算部5106は、乱数生成部5107で発生された乱数とベース格納部5109に格納され

ている秘密パラメータとから公開パラメータ（第1のシード生成情報、第5のシード生成情報）を計算する。また、ライセンス注入装置5003から転送されてくる第1のシード生成情報と乱数生成部5107で発生された乱数 $b_k$ とから第1のシードを生成する。またカードアダプタ5004から転送されてくる第5のシード生成情報と乱数生成部5107で発生された乱数 $d_k$ とから第5のシードを生成する。

【0500】共有鍵生成部5108には、鍵生成アルゴリズム $A_k(P_k)$ が予め格納されている。第1のシードにアルゴリズム $A_k(P_k)$ を適用して第1の共有鍵 $w_k1$ を生成し、第5のシードにアルゴリズム $A_k(P_k)$ を適用して第5の共有鍵 $w_l1$ を生成する。第1、第5のシードに鍵生成アルゴリズム $A_k(P_k)$ を適用することにより、第1、第5のシードのデータ長を小さくすることができる。KID格納部5105には、当該カードPを一意に識別するためのID（識別情報）、すなわち、KIDが予め格納されている。

【0501】KID暗号化部5104は、KID格納部5105に格納されているKIDを共有鍵生成部5108で生成された共有鍵 $w_k1$ 、 $w_k2$ で暗号化する。

【0502】制御部5103は、カードP全体の制御を司るものである。

【0503】(5-5) カードアダプタ

カードPは、カード装着部5004aに挿入される。カード装着確認部5004bにより、カードPが正常に装着されていることが確認されると、カードPとカードアダプタ5004とは、カード装着部5004aを介して通信可能な状態となる。

【0504】乱数生成部5004kは、AID格納部5004fに予め格納されている自身のID(AID)、ライセンス情報(Lic)、プレーヤにセットされたディスクDのID(DID)、カードPのID(KID)、ディスクキーの暗号化・復号化に用いる乱数 $b_l$ 、 $aD$ 、 $c_k$ 、 $dD$ を発生する。

【0505】乱数格納部5004lは、乱数生成部5004kで発生された乱数 $b_l$ 、 $aD$ 、 $c_k$ を記憶する。

【0506】ベース格納部5004mには秘密パラメータ $X(1)$ 、 $Pr1$ 、 $X(k)$ 、 $Prk$ 、 $X(D)$ 、 $PrD$ とが予め格納されている。

【0507】巾乗演算部5004jは、乱数生成部5004kで発生された乱数とベース格納部5004mに格納されている秘密パラメータとから公開パラメータ（第2、第4、第5、第6のシード生成情報）を計算する。また、カードPを介してライセンス注入装置5003から転送されてくる第2のシード生成情報と乱数生成部5004kで発生された乱数 $b_l$ とから第2のシードを生成する。また、カードPを介してライセンス注入装置5003から転送されてくる第3のシード生成情報と乱数生成部5004kで発生された乱数 $b_l$ とから第3のシ

ードを生成する。また、プレーヤ5005から転送されてくる第4のシード生成情報と乱数生成部5004kで発生された乱数 $aD$ とから第4のシードを生成する。また、カードPから転送されてくる第5のシード生成情報と乱数生成部5003kで発生された乱数 $c_k$ とから第5のシードを生成する。プレーヤ5005から転送されてくる第6のシード生成情報と乱数生成部5004kで発生された乱数 $dD$ とから第6のシードを生成する。

【0508】共有鍵生成部5004iには、鍵生成アルゴリズム $A_l(P_l)$ 、 $A_k(P_k)$ 、 $AD(PD)$ が予め格納されている。第2のシードにアルゴリズム $A_l(P_l)$ を適用して第2の共有鍵 $w_l1$ を生成し、第3のシードにアルゴリズム $A_l(P_l)$ を適用して第3の共有鍵 $w_l2$ を生成し、第4のシードにアルゴリズム $AD(PD)$ を適用して第4の共有鍵 $wD1$ を生成し、第5のシードにアルゴリズム $A_k(P_k)$ を適用して第5の共有鍵 $w_k2$ を生成し、第6のシードにアルゴリズム $AD(PD)$ を適用して第6の共有鍵 $wD2$ を生成する。第2～第6のシードに鍵生成アルゴリズム $A_l(P_l)$ 、 $A_k(P_k)$ を適用することにより、第2～第6のシードのデータ長を小さくすることができる。

【0509】暗号化／復号化部5004oは、共有鍵生成部5004iで生成された共有鍵 $wD2$ でディスクキーを暗号化する。また、共有鍵生成部5004iで生成された共有鍵 $w_l2$ 、 $wD1$ 、 $w_k2$ を用いて暗号化ライセンス情報[Lic] $w_l2$ 、暗号化ディスクID[DID] $wD1$ 、暗号化カードID[KID] $w_k2$ を復号する。

【0510】AID格納部5004fには、当該カードアダプタ5004を一意に識別するためのID（識別情報）、すなわち、AIDが予め格納されている。

【0511】AID暗号化部5004dは、AID格納部5004fに格納されているAIDを共有鍵生成部5004iで生成された共有鍵 $w_l1$ で暗号化する。

【0512】 $k_d$ 格納部5004gには、暗号化鍵 $k_e$ で暗号化されたディスク情報を復号するための復号化鍵 $k_d$ が格納されている。

【0513】プレーヤ接続部5004nには、プレーヤ5005がカードアダプタ5004と通信可能なように接続されている。

【0514】ライセンス判定部5004eは、カードPを介してライセンス注入装置5003から転送されてきたライセンス情報に含まれる暗号化ディスク情報を復号か鍵 $k_d$ で復号する。ライセンス判定処理(図139～図140)では、以下の条件をチェックする。・ライセンス情報に含まれるカードID(KID)およびカードアダプタID(AID)と、ライセンス判定部5004eに挿入されたカードPのカードID(KID)およびAID格納部5004fに格納されているカードアダプタID(AID)とが一致していること

・ライセンス情報の作成時刻が時計5004hの現在表示時刻より以前であること

・ディスク情報に含まれるディスクID(DID)とプレーヤ5005に現在セットされているディスクDのIDとが一致していること

・時計5004hの現在表示時刻がディスク情報に含まれる有効期限を満たすこと

以上の条件を満たすとき、ライセンス判定部5004eは、ディスク情報に含まれるディスクキーをプレーヤ5005へ出力する。その際、ディスクキーは、プレーヤ接続部5004nを介してプレーヤ5005との間で交換される第6のシード生成情報に基づき生成される共有鍵wD2で暗号化されている。

【0515】(5-6)プレーヤ

カードアダプタ接続部5005aには、カードアダプタ5004がプレーヤ5005と通信可能なように接続されている。

【0516】乱数生成部5005iは、ディスクドライブ5005dにセットされているディスクDから読み取ったディスクDのID(DID)、ディスクキーの暗号化・復号化に用いる乱数bD、cDを発生する。

【0517】乱数格納部5005kは、乱数生成部5005iで発生された乱数cDを記憶する。

【0518】ベース格納部5005lには秘密パラメータX(D)、PrDが予め格納されている。

【0519】巾乗演算部5005hは、乱数生成部5005iで発生された乱数とベース格納部5005lに格納されている秘密パラメータとから公開パラメータ(第4、第6のシード生成情報)を計算する。また、カードアダプタ5004から転送されてくる第4のシード生成情報と乱数生成部5005iで発生された乱bDとから第4のシードを生成する。また、カードアダプタ5004から転送されてくる第6のシード生成情報と乱数生成部5005iで発生された乱cDとから第6のシードを生成する。

【0520】共有鍵生成部5005jには、鍵生成アルゴリズムAD(PD)が予め格納されている。第4のシードにアルゴリズムAD(PD)を適用して共有鍵wD1を生成する。第6のシードにアルゴリズムAD(PD)を適用して共有鍵wD2を生成する。第4、第6のシードに鍵生成アルゴリズムAD(PD)を適用することにより、第4、第6のシードのデータ長を小さくすることができる。

【0521】ディスクドライブ5005dには、ディスクDがセットされて、ディスクDに記憶されているディスクID(DID)、暗号化コンテンツ情報、暗号化コンテンツキーが読み出される。ディスクID(DID)は、DID暗号化部5005cへ転送され、暗号化コンテンツ情報および暗号化コンテンツキーは再生部5005fへ転送される。

【0522】DID暗号化部5005cは、ディスクID(DID)を共有鍵生成部5005jで生成された共有鍵wD1暗号化する。

【0523】ディスクキー復号部5005eは、暗号化ディスクキー[ディスクキー]wD2を共有鍵生成部5005jで生成された共有鍵wD2で復号する。復号されたディスクキーは再生部5005fへ転送される。

【0524】再生部5005fは、暗号化コンテンツキーをディスクキーを用いて復号し、復号されたコンテンツキーを用いて暗号化コンテンツ情報を復号し、再生して、出力部5005gへ出力する。

【0525】(5-7)ディスクキーの配信手順(その1)

次に、図133に示すシーケンス図および図134～図140に示すフローチャートを参照して、図122の情報流通システムにおけるディスクキーの配信手順の概略をディスクレンタルサービスへの加入時、ディスクのレンタル時、コンテンツ再生時の順に説明する。

【0526】まず、ディスクレンタルサービスへの加入時について説明する。

【0527】ステップx1: ユーザに発行されるカードPは、ライセンス注入装置5003に挿入する。ライセンス注入装置5003は、乱数a1を発生する。カードアダプタ5004のID(AID)を取得するため、乱数a1と秘密パラメータ(X(1)、Pr1)とから、AIDを暗号化するために必要な公開パラメータ、すなわち、第2のシード生成情報 $X(1) \cdot a1 \pmod{Pr1}$ を計算し、カードPに転送する。(図134のステップS6001～ステップS6003)。

【0528】ステップx2: さらに、ライセンス注入装置5003は、乱数akを発生する。カードPのID(KID)を取得するために、乱数akと秘密パラメータ(X(k)、Prk)とから第1のシード生成情報 $X(k) \cdot ak \pmod{Prk}$ を計算し、カードPに転送する(図135のステップS6010～ステップS6011)。

【0529】ステップx3: カードPは、第1のシード生成情報を受け取り、乱数bkを発生する。乱数bkと第1のシード生成情報とから第1のシード $X(k) \cdot bk \pmod{Prk}$ を計算する。この第1のシードに、予め格納されているアルゴリズムAk(Pk)を適用して共有鍵wk1を生成する。共有鍵wk1を用いてカードPのID(KID)を暗号化する。以下、共有鍵wk1で暗号化されたKIDを[KID]wk1と記す。さらに、乱数bkと秘密パラメータ(X(k)、Prk)とから[KID]wk1を復号するために必要な第1のシード生成情報 $X(k) \cdot bk \pmod{Prk}$ を計算し、[KID]wk1と、この第1のシード生成情報とをライセンス注入装置5003へ転送する(図135のステップ

S6012～ステップS6016)。

【0530】ライセンス注入装置5003では、カードPから転送されてきた第1のシード生成情報と、先に発生した乱数 $a_k$ とから第1のシードを生成する。この第1のシードに、予め格納されているアルゴリズム $A_k$ ( $P_k$ )を適用して共有鍵 $w_{k1}$ を生成し、[KID] $w_{k1}$ を復号して、カードPのID(KID)を得る(ステップS6017～ステップS6019)。

【0531】このようにして取得されたカードPのIDは、カードデータベース(DB)5003iに、先に発生した乱数 $a_1$ に対応させて記憶される(図135のステップS6021)。カードDB5003iに記憶された情報は、後に、カードPを介して取得されるカードアダプタのID(AID)を復号する際に用いられる。この時点で、カードPには、ライセンス注入装置から受け取った第2のシード生成情報 $X(1)^{a_1} \pmod{Pr1}$ が格納されている。

【0532】ステップx4: ユーザは、以上の処理を施されたカードPを持ち帰り、自宅にあるカードアダプタ5004に当該カードPを挿入する。すると、カードアダプタ5004では、カードPから第2のシード生成情報を読み取る。また、カードアダプタ5004は、乱数 $b_1$ を発生し、この乱数 $b_1$ と第2のシード生成情報とから第2のシード $X(1)^{(a_1 \cdot b_1)} \pmod{Pr1}$ を計算する。この第2のシードに予め格納されているアルゴリズム $A_1(P_1)$ を適用して共有鍵 $w_{11}$ を生成する。そして、共有鍵 $w_{11}$ を用いて当該カードアダプタ5004の識別情報AIDを暗号化する。以下、共有鍵 $w_{11}$ で暗号化されたAIDを[AID] $w_{11}$ と記す。

【0533】ステップx5: 先に発生した乱数 $b_1$ と秘密パラメータ( $X(1)$ 、 $Pr1$ )とから第2のシード生成情報 $X(1)^{b_1} \pmod{Pr1}$ を計算し、この第2のシード生成情報と[AID] $w_{11}$ とをカードPに転送する(図134のステップS6004～ステップS6009)。

【0534】この時点で、カードPには、第2のシード生成情報と[AID] $w_{11}$ が記憶されていることになる。このとき、カードPでは、先に格納していた第2のシード生成情報 $X(1)^{a_1} \pmod{Pr1}$ を消去しても良い。カードアダプタ5004は、後にライセンス情報を復号する為に、乱数 $b_1$ を乱数格納部5004iに記憶しておく。

【0535】ユーザがディスクをレンタルしようとするときは、カードPを持参して、例えばディスクレンタルサービスの加盟店舗(ライセンス注入装置5003が設置されている店舗)に行き、所望のディスクを選択して、カードPとともに店員に差し出す。

【0536】ステップx6～ステップSx7: 差し出されたカードPとディスクDはライセンス注入装置50

03に挿入される。ライセンス注入装置5003は、当該カードPのID(KID)を取得するために、前述のステップx2～ステップx3と同様にして、カードPから当該カードPの識別情報を得る(図134のステップS6001、図135のステップS6010～ステップS6019)。なお、このとき発生される乱数 $a_k$ 、 $b_k$ は、前述のステップx2～ステップx3における乱数 $a_k$ 、 $b_k$ と必ずしも一致しないが、この事はKIDの取得に何ら影響を与えない。

【0537】ステップx8: カードPはライセンス注入装置5003へ第2のシード生成情報と[AID] $w_{11}$ を転送する。ライセンス注入装置5003は、カードDB5003iから、ステップx7で取得したカードID(KID)に対応する乱数 $a_1$ を検索する。前述した適正なる手続き処理を経たカードPであるならば、そのカードID(KID)に対応する乱数 $a_1$ がカードDB5003iに登録されているはずである。ライセンス注入装置5003は、カードPから転送された第2のシード生成情報と検索された乱数 $a_1$ とから第2のシード $X(1)^{(a_1 \cdot b_1)} \pmod{Pr1}$ を計算し、アルゴリズム $A_1(P_1)$ を適用する事によって、共有鍵 $w_{11}$ を生成する。共有鍵 $w_{11}$ を用いて[AID] $w_{11}$ を復号し、カードアダプタ5004のID(AID)を得る(図135のステップS6020～ステップS6021、図136のステップS6022～ステップS6026)。

【0538】ライセンス注入装置5003は、カードDB5003iに、このカードアダプタ5004の識別情報AIDをカードPの識別情報に対応させて記憶する(図136のステップS6027)。

【0539】かくして、ライセンス注入装置5003は、ユーザに与えられたカードID(KID)とカードアダプタID(AID)との組み合わせを把握する事ができる。ユーザが複数のカードアダプタを使用している様な場合でも、上記ステップx1～ステップx8の手続きにより、ライセンス注入装置5003は、ユーザの有する全てのカードアダプタのIDを把握する事ができる。その場合、カードDB5003iには、1つのカードID(KID)に対して複数のカードアダプタのID(AID)が対応付けられて記憶されることになる。

【0540】ステップx9: 一方、ライセンス注入装置5003は、挿入されたディスクDから当該ディスクのID(DID)を取得して、ライセンスDB5003fから当該ディスクIDに対応する暗号化ディスク情報を取得する。この暗号化ディスク情報に、時計5003hから取得した現在時刻をライセンス情報作成時刻としてマージし、カードDB5003iに含まれる情報(ユーザのカードID(KID)やカードアダプタID(AID))を必要に応じてマージしてライセンス情報(Lic)を作成する。すなわち、Lic=暗号化ディスク



情報+ライセンス情報作成時刻(+AID+KID)である。AID、KIDをライセンス情報Licに含めるか否かは、例えば、店舗の判断による。或いは、ライセンス作成装置5001がAID、KIDの要不要を決定し、その決定内容をライセンスDB5003fにカードIDに対応させて(付加情報として)記録して置いても良い(この場合、ライセンス注入装置5003は、この付加情報があれば、それに従ってAID、KIDをライセンス情報Licにマージするばよい)。ライセンス情報LicにAIDを含めるという事は、ライセンスを特定のカードアダプタに限定する事を意味する。又、ライセンス情報LicにKIDを含めるという事は、ライセンスを特定のカードに限定する事を意味する(図136のステップS6028～ステップS6030)。

【0541】さて、ライセンス注入装置5003は、乱数c1を発生する。カードPから既に第2のシード生成情報 $X(1)^{b1} \pmod{Pr1}$ を読み取っているから、ライセンス注入装置5003は、乱数c1とこの第2のシード生成情報とから第3のシード $X(1)^{(b1 \cdot c1)} \pmod{Pr1}$ を計算する。この第3のシードにアルゴリズムA1(P1)を適用して、鍵w12を生成して、ライセンス情報Licを暗号化する。以下、共有鍵w12で暗号化されたライセンス情報Licを[Lic]w12と記す。さらに、乱数c1と秘密パラメータ(X(1)、pr1)とから[Lic]w12を復号するために必要な公開パラメータ、すなわち、第3のシード生成情報 $X(1)^{c1} \pmod{Pr1}$ を計算し、この第3のシード生成情報と暗号化ライセンス情報[Lic]w12とをカードPに転送する(図136のステップS6031～ステップS6035)。この時点で、カードPには、暗号化ライセンス情報[Lic]w12と第3のシード生成情報とが記憶されていることになる。先にカードPに記憶されていた[AID]w11は、既にライセンス注入装置5003に渡されたので、消去されてもよい。

【0542】ユーザは、以上の処理を施されたカードPとディスクDとを持ち帰り、自宅にあるカードアダプタ5004、プレーヤ5005を用いてコンテンツの再生を行うことができる。

【0543】ステップx11: コンテンツを再生するために、ユーザがカードPをカードアダプタ5004へ挿入し、ディスクDをプレーヤ5005にセットする。カードアダプタ5004は、カードPから暗号化ライセンス情報[Lic]w12と第3のシード生成情報とを読み出し、この第3のシード生成情報とステップx5で一時格納された乱数b1とから第3のシード $X(1)^{(b1 \cdot c1)} \pmod{Pr1}$ を計算する。この第3のシードにアルゴリズムA1(P1)を適用して、共有鍵w12を生成し、暗号化ライセンス情報[Lic]w12を復号する(図138のステップS6046～

ステップS6049)。

【0544】ステップx12: 一方、プレーヤ5005は、セットされたディスクDからディスクID(DID)を読取る。

【0545】ステップx13: カードアダプタ5004は、乱数aDを発生する。カードアダプタ5004は、プレーヤ5005からこのディスクDのディスクID(DID)を取得するため、プレーヤ5005へディスクID(DID)を暗号化するために必要な公開パラメータ、すなわち、第4のシード生成情報を生成する。すなわち、乱数aDと、秘密パラメータ(X(D)、PrD)とから第4のシード生成情報 $X(D)^{aD} \pmod{PrD}$ を計算し、これをプレーヤ5005へ転送する(図137のステップS6036～ステップS6037)。

【0546】ステップx14: プレーヤ5005は、この第4のシード生成情報を受け取ると、乱数bDを発生し、第4のシード生成情報とこの乱数bDとから第4のシード $X(D)^{(aD \cdot bD)} \pmod{PrD}$ を計算し、アルゴリズムAD(PD)を適用して、共有鍵wD1を生成し、ディスクID(DID)を暗号化する。以下、共有鍵wD1で暗号化されたDIDを[DID]wD1と記す。さらに、乱数bDと秘密パラメータ(X(D)、PrD)とから[DID]wD1を復号するために必要な公開パラメータ、すなわち、第4のシード生成情報 $X(D)^{bD} \pmod{PrD}$ を計算し、[DID]wD1と、この第4のシード生成情報とをカードアダプタ5004へ転送する(図137のステップS6038～ステップS6042)。

【0547】カードアダプタ5004では、プレーヤ5005から転送されてきた第4のシード生成情報と[DID]wD1とを受け取ると、第4のシード生成情報と、乱数aDとから第4のシード $X(D)^{(aD \cdot bD)} \pmod{PrD}$ を計算する。この第4のシードにアルゴリズムAD(PD)を適用して共有鍵wD1を生成し、[DID]wD1を復号してディスクID(DID)を取得する(図137のステップS6043～ステップS6045)。

【0548】次に、図138のステップS6050に進み、ライセンス情報に基づくコンテンツ情報の復号可否を判定する処理(ライセンス判定処理)を行う(図139～図140)。

【0549】ライセンス情報にカードアダプタのIDが含まれている場合、カードアダプタ5004は、AID格納部5004fに格納されているカードアダプタID(AID)とライセンス情報に含まれているカードアダプタID(AID)とを比較する。これが一致しなければ、当該ライセンス情報は、当該カードアダプタ5004に適合するものではないので、処理を停止する。AIDが一致すれば、次の処理に進む(図139のステップ

S6061～ステップS6062)。

【0550】ステップx15: ライセンス情報にカードIDが含まれている場合、カードアダプタ5004は、カードPからその識別情報KIDを取得するため、まず、乱数ckを発生し、カードPのカードID(KID)を暗号化するために必要な公開パラメータ、すなわち、第5のシード生成情報を生成する。すなわち、乱数ckと秘密パラメータ(X(k)、Prk)とから第5のシード生成情報 $X(k)^{ck} \pmod{Prk}$ を計算し、カードPに転送する(図139のステップS6063～ステップS6065)。

【0551】ステップx16: カードPは、第5のシード生成情報を受け取ると、乱数dkを発生し、この第5のシード生成情報と乱数dkとから第5のシード $X(k)^{(ck \cdot dk)} \pmod{Prk}$ を計算する。第5のシードにアルゴリズムAk(Pk)を適用して、鍵wk2を生成し、カードPのカードID(KID)を暗号化する。以下、共有鍵wk2で暗号化されたKIDを[KID]wk2と記す。さらに、乱数dkから[KID]wk2を復号するために必要な公開パラメータ、すなわち、第5のシード生成情報 $X(k)^{dk} \pmod{Prk}$ を計算し、この第5のシード生成情報と[KID]wk2とをカードアダプタ5004へ転送する(ステップS6066～ステップS6070)。

【0552】カードアダプタ5004では、カードPから転送されてきた第5のシード生成情報と乱数ckとから第5のシードを計算する。この第5のシードにアルゴリズムAk(Pk)を適用して、鍵wk2を生成し、[KID]wk2からKIDを復号する。このカードPから送られてきたカードID(KID)と、ライセンス情報に含まれていたカードID(KID)とが一致する場合、次の処理に進む。さもなければ、カードPに記憶されていたライセンス情報が当該カードPに不適合であったわけであるから、以後の処理を停止する(ステップS6071～ステップS6074)。

【0553】ステップx17: 次に、カードアダプタ5004は、ライセンス情報に含まれるライセンス情報作成時刻をチェックする。ライセンス情報作成時刻をT1と表す事にする。カードアダプタ5004は時計5004hから現在表示時刻Tcを取得する。 $Tc \leq T1$ のときは現在表示時刻Tcが遅れている事を示している。実際、ライセンス情報が作成された時刻T1は、現在表示時刻Tcよりも前であればならない筈である。従って、 $Tc \leq T1$ のときは、カードアダプタ5004は、時計5004hが不正確であると判断し、以後の処理を停止する。或いは、若干の許容誤差範囲Te(>0)を予め設定しておき、 $Tc > T1 + Te$ が成立する時及びその時に限って、以後の処理に進む様にしても良い(図140のステップS6075)。

【0554】次に、予め保持されていた復号化鍵kdを

用いてライセンス情報に含まれていた暗号化ディスク情報を復号する(ステップS6076)。ディスク情報には、ディスクID(DID)、ディスクキー、有効期限(TL)とが含まれている。まず、有効期限TLと時計6004hの現在表示時刻Tcとを比較する。 $TL < Tc$ であれば、ライセンスは有効期限は切れているので、カードアダプタ5004は以後の処理を停止する。或いは、若干の許容誤差Te'(>0)を予め設定しておき、 $Tc \leq TL + Te'$ が成立する時及びその時に限って、以後の処理に進む様にしても良い(ステップS6077)。

【0555】最後に、カードアダプタ5004は、ディスク情報に含まれるディスクID(DID)と、先を取得したディスクDのディスクIDとを比較して、両者が一致しなければ、当該ライセンス情報は、現在プレーヤ5005にセットされているディスクDとは異なるディスクに対するものであるから、以後の処理を中止する。ディスクIDが一致した場合に、当該ディスクDに記録されているコンテンツ情報の再生が可能と判定される(ステップS6078)。

【0556】再生可と判定されたとき、カードアダプタ5004は、ディスク情報に含まれていたディスクキーをプレーヤ5005へ転送するため、まず、プレーヤ5005に対して、乱数の発生を指示する。

【0557】ステップx18: 乱数発生を指示を受けたプレーヤ5005は、乱数cdを発生し、この乱数cdと秘密パラメータ(X(D)、PrD)とから第6のシード生成情報 $X(D)^{cd} \pmod{PrD}$ を計算し、カードアダプタ5004に転送する(図138のステップS6051～ステップS6052)。

【0558】ステップx19: カードアダプタ5004は、第6のシード生成情報を受け取ると、乱数ddを発生する。第6のシード生成情報と乱数ddとから第6のシード $X(D)^{(cd \cdot dd)} \pmod{PrD}$ を計算し、この第6のシードにアルゴリズムAD(PD)を適用して、ディスクキー暗号化用の共有鍵wd2を生成し、ディスクキーを共有鍵wd2で暗号化する。以下、共有鍵wd2で暗号化されたディスクキーを[ディスクキー]wd2と記す。さらに、乱数ddと秘密パラメータ(X(D)、PrD)とから[ディスクキー]wd2を復号するために必要な公開パラメータ、すなわち、第6のシード生成情報 $X(D)^{dd} \pmod{PrD}$ を計算し、この第6のシード生成情報と[ディスクキー]wd2とをプレーヤ5005へ転送する(ステップS6053～ステップS6056)。

【0559】プレーヤ5005では、カードアダプタ5004から転送されてきた第6のシード生成情報と乱数cdとから第6のシード $X(D)^{(cd \cdot dd)} \pmod{PrD}$ を計算する。この第6のシードに、アルゴリズムAD(PD)を適用して、共有鍵wd2を生成

し、[ディスクキー] wD2を復号する(ステップS6057～ステップS6059)。

【0560】プレーヤ5005は、このディスクキーを用いて、ディスクDに記憶されている暗号化コンテンツキーを復号し、さらに、このコンテンツキーで暗号化コンテンツ情報の復号・再生を行うことができる(ステップS6060)。

【0561】なお、暗号化ディスク情報の復号化鍵Kdをプレーヤ5005に格納する事も可能である。この場合、暗号化ディスク情報を復号するのはプレーヤ5005である。ライセンス情報作成時刻、有効期限等の有効性を判定するために参照される時計5004hはカードアダプタ5004であるので、有効期限を暗号化ディスク情報に含めることができない。従って、このような場合、ライセンス作成装置5001からライセンス注入装置5003に転送される暗号化ディスク情報の構成要素は、「ディスクID+ディスクキー」となる。有効期限は、ライセンス注入装置5003が設定し、前述のステップx9でライセンス情報の作成する際に、暗号化ディスク情報に有効期限をマージして、暗号化ディスク情報、ライセンス情報作成時刻、有効期限、必要に応じてカードID(KID)とカードアダプタID(AID)を含むライセンス情報を作成すればよい。

【0562】カードアダプタ5004では、復号化鍵Kdによるディスク情報の復号を行うことなく有効期限の有効性を判定する。

【0563】復号化鍵Kdをプレーヤ5005に保持させるメリットは、

- ・ライセンス注入装置5003に蓄積される暗号化ディスク情報が有効期限を含んでいない為、ディスク情報を更新する必要がない。すなわち、ライセンス作成装置5001は新たに追加されたレンタル用のディスクの暗号化ディスク情報だけを作成し、ライセンス注入装置5003へ適宜転送すれば良い。

【0564】一方、デメリットは、

- ・暗号化ディスク情報が更新されることがないので、ライセンス注入装置5003の不正使用に対する動機を強めてしまう。

【0565】・プレーヤ5005内の復号化鍵Kdを保護する為に、プレーヤ5005のセキュリティを高めないてはならない。

【0566】さて、以上のディスクキーの配信手順によれば、ユーザが行う手順を簡単に説明する。

【0567】i) ディスクレンタルサービスへの加入時に、ユーザは、当該ディスクレンタルサービスの加盟店舗でカードPの発行を受ける。場合によっては、この際にカードアダプタ5004を購入する、又はカードアダプタ5004の貸与を受ける。

【0568】ii) ユーザが自宅でプレーヤ5005に接続されたカードアダプタ5004にカードPを挿入す

る。

【0569】iii) ユーザがディスクをレンタルするときには、カードPをもって、店舗に赴き、所望のレンタルディスクDを選択し、代金と引き換えに、カードPにライセンスの注入を受ける。

【0570】iv) ユーザがディスクDとカードPとを自宅に持ち帰り、カードアダプタ5004にカードPを挿入して、ディスクDを再生する。ライセンス有効期間中、ディスクDを幾度でも再生する事ができる。

【0571】v) 以後、ユーザがディスクをレンタルする際には、上記iii)～iv)を繰り返す。

【0572】(5-8) ディスクキーの配信手順(その2)

ところで、ディスクレンタルサービスへの加入時に、カードPの発行を受けると同時に、ディスクがレンタルできれば、一層ユーザにとって便利である。この場合のユーザが行う手順を簡単に説明する。

【0573】i) ディスクレンタルサービスへの加入時に、ユーザは、当該ディスクレンタルサービスの加盟店舗でカードPの発行を受ける。場合によっては、この際にカードアダプタ5004を購入する、又はカードアダプタ5004の貸与を受ける。

【0574】ii') ユーザは、所望のレンタルディスクDを選択し、代金と引き換えに、カードPにライセンスの注入を受ける。

【0575】iii') ユーザは、ディスクDとカードPとを自宅に持ち帰り、カードアダプタ5004にカードPを挿入して、ディスクDを再生する。ライセンス有効期間中、ディスクを幾度でも再生する事ができる。

【0576】iv') 以後、ユーザがディスクをレンタルする際には、上記ii')～iii')を繰り返す。

【0577】次に、このような場合のディスクキーの配信手順について説明する。

【0578】図141に示すシーケンス図および図142～図146に示すフローチャートを参照して、図122の情報流通システムにおけるディスクキーの他の配信手順の概略をディスクレンタルサービスへの加入・ディスクのレンタル時、コンテンツ再生時の順に説明する。

【0579】ディスクレンタルサービスに加入しているユーザに提供される全てのカードアダプタ5004およびライセンス注入装置5003は、乱数b10を共有している。乱数b10は、例えばROM等に記憶されていて、カードアダプタ外部から読み出すのは困難なように保護されていることが望ましい。

【0580】乱数b10は、ライセンス注入装置5003、カードアダプタ5004のそれぞれのベース格納部5003m、5004mに予め格納されているものとする。まず、ディスクレンタルサービスへの加入時について説明する。

【0581】ステップy1～ステップy2: ユーザに

発行されるカードPは、ライセンス注入装置5003に挿入する。ライセンス注入装置5003は、図133のステップx2～ステップx3、ステップx6～ステップx7と同様にして、カードPからカードID(KID)を取得する(図142のステップS6101～ステップS6110)。

【0582】ステップy3: ユーザにより選択されたレンタルディスクDもライセンス注入装置5003に挿入される。ライセンス注入装置5003は、挿入されたディスクDから当該ディスクのID(DID)を取得して、ライセンスDB5003fから当該ディスクIDに対応する暗号化ディスク情報を取得する。

【0583】ライセンス注入装置5003は、時計5003hから取得した現在時刻をライセンス情報作成時刻としてマージし、さらに、ユーザのカードID(KID)をマージしてライセンス情報(Lic)を作成する(図142のステップS6111～ステップS6114)。すなわち、

$Lic = \text{暗号化ディスク情報} + \text{ライセンス情報作成時刻} + KID$

である。

【0584】ステップy4: 次に、ライセンス注入装置5003は、乱数a1を発生する。そして、カードDB5003iにカードPのカードIDと乱数a1とを記憶する。

【0585】乱数a1と例えば、秘密パラメータ(X(1)、pr1)とから第7のシード $X(1)^{(a1 \cdot b10)} \pmod{Pr1}$ を計算し、さらに、この第7のシードにアルゴリズムA1(P1)を適用して、共有鍵w13を生成し、ライセンス情報Licを暗号化する。以下、共有鍵w13で暗号化されたライセンス情報Licを[Lic]w13と記す。さらに、乱数a1と秘密パラメータ(X(1)、pr1)とから[Lic]w13を復号するために必要な公開パラメータ、すなわち、第7のシード生成情報 $X(1)^{a1} \pmod{Pr1}$ を計算し、この第7のシード生成情報と暗号化ライセンス情報[Lic]w13とをカードPに転送する(図142のステップ6115～ステップx6119)。

【0586】この時点で、カードPには、暗号化ライセンス情報[Lic]w13と第7のシード生成情報とが記憶されていることになる。

【0587】ユーザは、以上の処理を施されたカードPとディスクDとを持ち帰り、自宅にあるカードアダプタ5004、プレーヤ5005を用いてコンテンツの再生を行うことができる。

【0588】ステップy5: コンテンツを再生するために、ユーザがカードPをカードアダプタ5004へ挿入し、ディスクDをプレーヤ5005にセットする。カードアダプタ5004は、カードPから暗号化ライセン

ス情報[Lic]w13と第7のシード生成情報とを読み出し、この第7のシード生成情報とベース格納不5004mに予め格納された乱数b10とから第7のシード $X(1)^{(a1 \cdot b10)} \pmod{Pr1}$ を計算する。この第7のシードにアルゴリズムA1(P1)を適用して、共有鍵w13を生成し、暗号化ライセンス情報[Lic]w13を復号する。カードアダプタ5004は、さらに、ライセンス情報に含まれていた暗号化ディスク情報を復号化鍵Kdで復号する(図143のステップS6120～ステップS6129)。

【0589】ステップy8～ステップy9: カードアダプタ5004は、図133のステップx15～ステップx16と同様にしてカードPからカードID(KID)を取得する(図143のステップS6130～ステップS6139)。

【0590】ステップy10～ステップy12: カードアダプタ5004は、さらに、図133のステップx12～ステップx14と同様にしてディスクDのディスクID(DID)を取得する(図144のステップS6140～ステップS6149)。

【0591】ステップy13: 次に、図145のステップS6150に進み、ライセンス情報に基づくコンテンツ情報の復号可否を判定する処理(ライセンス判定処理)を行う(図146)。

【0592】ライセンス判定処理(図146)では、以下の条件をチェックする。

- ・ライセンス情報に含まれるカードID(KID)と、カードアダプタ5004に挿入されたカードPのカードIDとが一致していること
- ・ディスク情報に含まれるディスクID(DID)とプレーヤ5005に現在セットされているディスクDのディスクIDとが一致していること
- ・ライセンス情報の作成時刻が時計5004hの現在表示時刻より以前であること
- ・時計5004hの現在表示時刻がディスク情報に含まれる有効期限を満たすこと

以上の条件を満たすときのみ、カードアダプタ5004は、当該ディスクDに記録されているコンテンツ情報の再生が可能であると判定し、ディスク情報に含まれていたディスクキーをプレーヤ5005へ転送するため、まず、プレーヤ5005に対して、乱数の発生を指示する。

【0593】ステップy14～ステップy15: 図133のステップx18～ステップx19と同様にして、ディスクキーは、プレーヤ5005との間で交換される第6のシード生成情報に基づき生成される共有鍵wD2で暗号化されて、プレーヤ5005へ転送される(図145のステップS6150～ステップS6161)。ステップy6～ステップy7: 一方、カードアダプタ5004は、上記ライセンス判定処理に前後して、カー

ドPにAID格納部5004fに予め格納されているカードアダプタID(AID)を転送する処理を実行する。その際、カードアダプタID(AID)は、図133のステップx4～ステップx5と同様にして、カードPを介してライセンス注入装置5003から転送されてきた第7のシード生成情報(第2のシード生成情報と同じもの)と、乱数生成部5004kで発生した乱数b1とに基づき生成される共有鍵w11で暗号化される。

【0594】2回目のディスクレンタル時以降は、図133のステップx6～ステップx19と同様である。なお、2回目のディスクレンタル時に、ライセンス注入装置5003は、図133のステップx8でユーザの所持するカードアダプタのID(AID)を取得することができる。すなわち、カードDB5003iにカードPのカードID(KID)とカードアダプタID(AID)との対応関係が登録される。

【0595】(5-9)暗号パラメータの更新  
本発明のディスクキーを含むライセンス情報の配信は、配信経路上の各装置の持つ秘密パラメータと各装置間で交換される(秘密パラメータから生成される)公開パラメータとに基づき相手認証と転送保護とを行っている。従って、定期的に、或いはセキュリティに対する攻撃の疑いがある場合に適宜、秘密パラメータや暗号化ディスク情報の復号化鍵kd等(以下、これらをまとめて暗号パラメータと呼ぶ)を更新する事が望ましい。この更新は、ライセンス作成装置5001が主導して行うことが望ましい。

【0596】ライセンス作成装置5001が更新する暗号パラメータは、例えば、 $(X(1), P1, Pr1)$   $(X(k), Pk, Prk)$   $(X(D), PD, PrD)$   $(Kd, Ke)$  であるとして、図147～図149に示すフローチャートを参照して、暗号パラメータ更新処理について説明する。

【0597】ライセンス作成装置5001の暗号パラメータ生成部5001hでは、上記暗号パラメータを例えば乱数発生器等を用いて更新する。次いで、各装置(プレーヤ5005、カードアダプタ5004、カードP、ライセンス注入装置5003)用にパラメータ更新情報を作成する(図147のステップS6201)。

【0598】プレーヤ用パラメータ更新情報は、 $X(D)$ 、 $PD$ 、 $PrD$ を含み、カードアダプタ用パラメータ更新情報は $X(1)$ 、 $P1$ 、 $Pr1$ 、 $X(k)$ 、 $Pk$ 、 $Prk$ 、 $X(D)$ 、 $PD$ 、 $PrD$ 、 $Kd$ を含み、カード用パラメータ更新情報は $X(k)$ 、 $Pk$ 、 $Prk$ を含み、ライセンス注入装置用パラメータ更新情報は $X(1)$ 、 $P1$ 、 $Pr1$ 、 $X(k)$ 、 $Pk$ 、 $Prk$ を含む。

【0599】第2の暗号化部5001gは、各装置用のパラメータ更新情報を、第2の暗号鍵格納部5001fに予め格納されている暗号化鍵KsD、KsA、Ks

C、KsLでそれぞれ暗号化する(ステップS6202～ステップS6203)。すなわち、プレーヤ用パラメータ更新情報は暗号鍵KsDで暗号化し、カードアダプタ用パラメータ更新情報は暗号鍵KsAで暗号化し、カード用パラメータ更新情報は暗号鍵KsPで暗号化し、ライセンス注入装置用パラメータ更新装置は暗号鍵KsLで暗号化する。以下、各装置用のそれぞれに対応した暗号化鍵で暗号化されたパラメータ更新情報を、例えば、プレーヤ用暗号パラメータの場合、[パラメータ更新情報]KsDと表す。

【0600】各装置用の暗号化パラメータ更新情報を以下に示す。

【0601】プレーヤ用の暗号化パラメータ更新情報(UD):  $[X(D) + PD + PrD] KsD$

カードアダプタ用の暗号化パラメータ情報(UA):  $[X(1) + P1 + Pr1 + X(k) + Pk + Prk + X(D) + PD + PrD + Kd] KsA$

カード用の暗号化パラメータ情報(UC):  $[X(k) + Pk + Prk] KsC$

ライセンス注入装置用の暗号化パラメータ情報(UL):  $[X(1) + P1 + Pr1 + X(k) + Pk + Prk] KsL$

時計5001aから現在表示時刻(暗号パラメータ更新時刻)を取得し、それを上記各装置用の暗号化パラメータ情報とともに、ライセンス注入装置5003へ転送する(ステップS6204～ステップS6205)。

【0602】ライセンス注入装置は、各装置用の暗号化パラメータ情報(UD、UA、UC、UL)と更新時刻とを受信すると、暗号化パラメータ情報UD、UA、UC及び更新時刻を内部メモリに格納する(図148のステップS6206)。

【0603】ライセンス注入装置5004は、暗号化鍵KsLに対応する復号化鍵KpLを予めメモリに記憶しており、この復号化鍵KpLを用いて暗号化パラメータ更新情報ULを復号し、ベース格納部5003m、共有鍵生成部5003lに記憶されている暗号パラメータ $X(1)$ 、 $P1$ 、 $Pr1$ 、 $X(k)$ 、 $Pk$ 、 $Prk$ を更新する(ステップS6208)。なお、 $P1$ 及び $Pk$ は、夫々鍵生成アルゴリズムA1、Akのパラメータであったから、鍵生成アルゴリズムが更新される事になる。

【0604】カードPの暗号パラメータの更新処理動作は、カードPがライセンス注入装置5003に挿入された際、実行される。

【0605】ユーザの所持するカードPがライセンス注入装置5003に挿入されると、ライセンス注入装置5003は、カードPから最新の暗号パラメータ更新時刻を取得する。この更新時刻が、ライセンス注入装置5003に格納されている更新時刻(ライセンス作成装置5001から転送されてきた更新時刻)より古いとき、ステップS6210へ進み、それ以外ときは、暗号パラメ

ータ更新動作は終了し、ライセンス情報の書き込み等、通常の処理動作を行う（ステップS6209）。ステップS6210では、ライセンス注入装置5003は、暗号化パラメータ更新情報UD、UA、UCおよび更新時刻をカードPに転送する。カードPは、暗号化パラメータ更新情報UD、UA及び更新時刻を内部メモリに格納する。

【0606】カードPは、暗号化鍵KsCに対応する復号化鍵KpCを予めメモリに記憶しており、この復号化鍵KsCを用いて暗号化パラメータ更新情報UCを復号し、ベース格納部5109、共有鍵生成部5108に記憶されている暗号パラメータX(k)、Pk、Prkを更新する（ステップS6211～ステップS6212）。その後、通常の処理動作を行う。

【0607】カードアダプタ5004の暗号パラメータの更新処理動作は、ユーザがカードPをカードアダプタ5004に挿入した際に実行される。すなわち、カードアダプタID(AID)をカードPに転送する際、あるいは、ディスクDを再生する為にカードPからカードアダプタ5004へライセンス情報を転送する際に、カードアダプタ5004の暗号パラメータの更新処理が実行される。

【0608】カードPは、まず、カードPの最新の暗号パラメータ更新時刻（ライセンス有入装置5003から転送されてきた更新時刻）をカードアダプタ5004へ転送する。カードアダプタ5004は、この更新時刻がカードアダプタ5004が記憶している最新の暗号パラメータの更新時刻より古いときはステップS6214へ進み、それ以外のときは、暗号パラメータ更新動作は終了し、通常の処理動作を行う（ステップS6213）。

【0609】ステップS6214では、カードPは、暗号化パラメータ更新情報UD、UA及び更新時刻、カードアダプタ5004へ転送する。カードアダプタ5004は、UD及び更新時刻を内部メモリに格納する。

【0610】カードアダプタ5004は、暗号化鍵KsAに対応する復号化鍵KpAを予めメモリに記憶しており、この復号化鍵KpAを用いて暗号化パラメータ更新情報UAを復号し、ベース格納部5109、共有鍵生成部5108、kd格納部5004gに記憶されている暗号パラメータX(1)、P1、Pr1、X(k)、Pk、Prk、X(D)、PD、PrD及びKdを更新する（ステップS6215～ステップS6216）。その後、通常の処理動作を行う。

【0611】プレーヤ5005の暗号パラメータの更新処理動作は、カードアダプタ5004とプレーヤ5005とが通信を行うとき実行される。すなわち、例えば、プレーヤ5005からカードアダプタ5004に対してディスクID(DID)を転送する際に、プレーヤ5005の暗号パラメータの更新処理が実行される。

【0612】例えば、プレーヤ5005がカードアダプ

タ5004にディスクID(DID)を転送する前に、まず、プレーヤ5005の最新の暗号パラメータの更新時刻をカードアダプタ5004へ転送する。

【0613】カードアダプタ5004は、プレーヤ5005から転送されてきた更新時刻がカードアダプタ5004が記憶している最新の暗号パラメータの更新時刻より古いときは、ステップS6218へ進み、それ以外のときは、暗号パラメータ更新動作は終了し、通常の処理動作を行う（ステップS6217）。

【0614】ステップS6218では、カードアダプタ5004は、暗号化パラメータ更新情報UD及び更新時刻をプレーヤ5005へ転送する。プレーヤ5005は、更新時刻を内部メモリに格納する。

【0615】プレーヤ5005は、暗号化鍵KsDに対応する復号化鍵KpDを予めメモリに記憶しており、この復号化鍵KpDを用いて暗号化パラメータ更新情報UDを復号し、ベース格納部5005i、共有鍵生成部5005jに記憶されている暗号パラメータX(D)、PD、PrDを更新する（ステップS6219～ステップS6220）。その後、通常の処理動作を行う。

【0616】以上が、暗号パラメータの更新処理動作が終了する。暗号パラメータの更新は、ライセンス注入装置5003に挿入される全てのカード（ユーザに発行された全てのカード）に対して行われる。従って、暗号パラメータの更新は、暗号パラメータの更新されたカードPが挿入される全てのカードアダプタ5004および該カードアダプタ5004に接続されているプレーヤ5005の全てに波及する。

【0617】(5-10) ディスクキーの配信手順(その3)

カードアダプタ5004とプレーヤ5005とが1つの装置として構成されている場合もあり得る（以下、第2のプレーヤと呼ぶ）。この場合のディスクキーを含めたライセンス情報の配信手順について、図133、図141を参照して簡単に説明する。すなわち、図133において、カードアダプタ5004とプレーヤ5005との間のディスクIDの転送処理（ステップx13～ステップx14）とディスクキーの転送処理（ステップx18～ステップx19）が不要となる。また、ステップx5において、カードPを経由してライセンス注入装置5003へ転送されるカードアダプタIDは、第2のプレーヤのID(PID)である。

【0618】図141においてもカードアダプタ5004とプレーヤ5005との間のディスクIDの転送処理（ステップy11～ステップy12）とディスクキーの転送処理（ステップy14～ステップy15）が不要となる。また、ステップy7において、カードPを経由してライセンス注入装置5003へ転送されるカードアダプタIDは、第2のプレーヤのID(PID)である。

【0619】それ以外は、前述同様である。

【0620】以上説明したように、上記第5の実施形態によれば、コンテンツ情報を復号するために必要なディスクキーを、その配信元（ライセンス作成装置、ライセンス注入装置）から配信先（カードアダプタ、プレーヤ）までの安全に配信することができる。

（第6の実施形態）図150は、本発明の第6の実施形態に係る情報流通システムの構成例を示したもので、課金対象である暗号化されたコンテンツ情報（著作物）は、DVD等の情報記録メディア（以下、簡単にディスクと呼ぶ）7103に予め記録されており、ディスク7103に記録されているコンテンツ情報を再生可能にするライセンスを購入して、あるいは、当該コンテンツ情報の利用に対する点数（ポイント）を予め購入して、当該ディスク7103を貸し出すことによりなるレンタルサービスを提供するためのものである。すなわち、利用料金と引き換えにライセンス情報を提供する前述の実施形態で説明したようなライセンス方式とポイント方式とを組み合わせた超流通を実現することができる情報流通システムである。ポイント方式とは、プリペイドカード等に注入された著作物利用権をポイントとして利用者が予め購入しており、著作物の利用と引き換えに当該ポイントを減点する方式を言う。ポイント減点の際に著作物利用の明細（著作物のIDなど）をカードに記録し、カード回収の際に明細を回収し、プリペイドカード販売による収益の分配等に利用する方式を超流通と呼ぶ。

【0621】ポイント方式は、ライセンス方式と比較して、次のメリットを有する。すなわち、予め店舗等で著作物の利用権であるポイントを購入しておけば、店舗にわざわざ出向くこと無く、著作物の利用ポイントと引き換えに、著作物を利用する事が可能である。

【0622】ライセンス方式の場合でも、再生装置がライセンスサーバ（ライセンスの発行装置）と通信回線等を経由して接続可能であれば、店舗に出向くこと無く、著作物の利用権を入手する事は可能である。即ち、何らかのオンライン課金方式を利用して代金を支払い、ライセンス情報を入手すれば良い。ポイント方式のメリットは、オフライン（ライセンスサーバと接続されていない）状態で、著作物利用ポイントの減点による著作物利用権の取得が可能であるという点にある。

【0623】一方、ポイント方式は、ライセンス方式と比較して、次のデメリットを有する。すなわち、著作物利用ポイントは、一種の著作物利用権購入用の金銭あるいは商品券であり、個別著作物のライセンスよりも、汎用的に使用可能である。従って、ライセンス方式よりも不正利用への動機付けが強い。ポイント方式のデメリットは、著作物利用ポイントの汎用性（例えば、利用権を購入した会員が利用する可能性のある再生装置以外の再生装置にも利用可能であるということ）に由来している。

【0624】今、著作物レンタル業者により発行された

レンタル会員カード7102に、著作物利用ポイントを記録する場合を考える。当該著作物利用ポイントを含む機密性を有する情報（以下、ポイント情報と呼ぶ）の不正コピーなどを防止する観点から、会員カード7102に記録されるポイント情報は、会員が利用する再生装置が、そして当該再生装置のみが読み取り可能である事が望ましい。ところが、店舗で会員カードにポイント情報を記録する際に、会員が利用する可能性のある再生装置を特定する情報（再生装置のIDなど）を取得して、当該ポイント情報に組み込むことは、一般に不可能である。

【0625】そこで、第6の実施形態では、ライセンス方式とポイント方式とを組み合わせる使用することによって、それぞれの方式のメリットを活かしつつ、デメリットを解消するものである。

【0626】図150において、当該情報流通システムにより新規入会会員が、著作物情報（コンテンツ情報）が記録されたディスク7103を購入する（著作物利用権は購入代金に含まれていない）際には、ライセンス方式によって当該著作物のライセンス情報を取得する。即ち、ディスク7103とは別途当該著作物のライセンス情報を購入する。

【0627】当該ディスク7103再生時に、会員の再生装置7101は会員カード7102からライセンス情報を読み取るが、その際、再生装置7101は、当該再生装置7101を一意的に特定でき、しかも、一度限り使用する情報（例えば、暗号鍵、乱数）Rをカードに記録する。

【0628】会員は、次回の利用権購入からは、ライセンス情報の購入とともに、あるいはライセンス情報の購入に代えて、ポイント方式を利用する事が可能である。すなわち、2回目以降の利用権購入の際に、ポイント方式を利用する場合、店舗のライセンス／ポイント注入装置7111は、会員カード7102から情報Rを読み取り、情報Rを利用して、当該再生装置7101のみが利用できる形で、ポイント情報を会員カード7102に記録する。

【0629】当該会員が再生装置7101にポイント情報が記録された会員カード7102を挿入すると、再生装置7101は会員カード7102からポイント情報を読み取り、その中に含まれるポイントを再生装置7101に格納する。ディスク7103を再生する際に、再生装置7101は当該格納したポイントから然るべき点数を減じる。

【0630】なお、センター装置7121は、ライセンス／ポイント注入装置7111からの要求に応じて、ライセンス情報およびポイント情報を発行し、それを要求元のライセンス／ポイント注入装置7111に送信する。ライセンス／ポイント注入装置7111はセンター装置7121から送信されてきたライセンス情報、ポイ

ント情報を会員カード7102に記録するようになって  
いる。

【0631】このようなシステムにより、

- ・ 会員カードに記録されたポイントの利用が、特定の再生装置（当該会員の利用する可能性のある再生装置）に限定することができる

- ・ 会員カードに記録されたポイント情報を最初に読み取った再生装置にのみ当該著作物の利用を限定することができる。

【0632】従って、著作物利用に対し発行されるポイントの汎用性を限定することができる。

【0633】この様に、図150の情報流通システムは、ポイント方式を採用するにあたり、そのポイントの不正利用に対処しシステムの安全性を向上させるとともに、利用者の便宜を殆ど損なう事が無い。ポイント方式の利用が制限されるのは新規入会時のみであり、以後はポイント方式とライセンス方式の両方式が利用可能である。すなわち、会員カード7102にライセンス情報とポイント情報のいずれか一方が記録される場合もあるし、双方が共に記録される場合もある。後者の場合は、ライセンス情報を優先的に用いることが望ましい。

【0634】以下、図151を参照して、レンタルサービス提供のために、ディスク7103、会員カード7102、再生装置7101のそれぞれにおいて用いられる情報データについて説明する。

【0635】ディスク7103には、

- ・ 課金対象の著作物であるコンテンツ情報をタイトルキーKTで暗号化したもの（[コンテンツ情報]KT）
- ・ コンテンツの識別情報（コンテンツID）
- ・ タイトルキーKTをディスクキーKDで暗号化したもの（[KT]KD）
- ・ ディスクキーKDをマスターキーKMで暗号化したもの（[KD]KM）をさらにレンタルキーKRで暗号化したもの（[[KD]KM]KR）
- ・ レンタルキーKRを複数の暗号用ライセンスキー（公開鍵）KLP(j)（j=1、2、3…）のそれぞれで暗号化したもの（[KR]KLP(1)、[KR]KLP(2)、[KR]KLP(3)、…）

タイトルキーKTは、コンテンツ情報の1タイトル毎に予め定められた暗号鍵である。

【0636】ディスクキーKDは、各ディスク毎に定められた暗号鍵である。

【0637】マスターキーKMは、当該サービスに加入している会員にのみに与えられる暗号化復号化鍵で、図152の再生装置7101の第3の復号部7101iに格納されている。

【0638】レンタルキーKRは、コンテンツ情報を復号する際に必要となる暗号化復号化鍵で、例えば、同時期に製造されたディスク7103には同一のレンタルキーが用いられる。

【0639】暗号用ライセンスキーKLP(1)、KLP(2)、KLP(3)、…のそれぞれに対応する復号用ライセンスキーKLS(j)は、レンタル時に会員カード7102に記録されるポイント情報に含まれている。

【0640】異なる複数の暗号用ライセンスキーKLP(1)、KLP(2)、KLP(3)、…によって、レンタルキーKRを暗号化したものが複数ディスク7103に記録されているのは、適宜復号用ライセンスキーKLS(j)を変更する事を可能にする為である。暗号用ライセンスキーKLP(j)によって暗号化されたレンタルキーKRは、復号用ライセンスキーKLS(j)によって復号することができる。

【0641】ライセンス情報(CL)は、他の実施形態で述べたライセンス情報と同様で、例えば、レンタルキーKR、ライセンス情報作成日時、利用条件等がマージされ、その全体が暗号化鍵Ksで暗号化されている。すなわち、

暗号化ライセンス情報([CL]Ks)=[レンタルキーKR+ライセンス情報作成日時+利用条件]Ks

と表すことができる。ライセンス情報(CP)は、会員カードに複数記録されている事もある。

【0642】ポイント情報は、

- ・ ポイントと認証情報Apとをマージしたものを暗号鍵Ktで暗号化したもの（[ポイント+Ap]Kt）

- ・ 複数の復号用レンタルキーKLS(j)のうちの1つと、その識別子jとをマージし、全体を暗号化鍵ksで暗号化されている。すなわち、

暗号化ポイント情報([CP]Ks)=[ [ポイント+Ap]Kt+j+KLS(j) ] Ks

と表すことができる。

【0643】暗号鍵ktは、再生装置7101（図152の一時鍵発生部7101f）にて発生される暗号鍵で、当該再生装置7101を一意的に特定でき、しかも、一度限り使用する（ここでは、1つのポイント情報を作成する際に用いられる）情報Rに相当するものである。すなわち、異なる再生装置からは異なる暗号鍵ktが発生する。従って、[ポイント+Ap]Ktを復号するには、当該暗号鍵ktを発生した再生装置のみが行える。

【0644】認証情報Apは、当該ポイント情報が正当なものであるか否か（センター装置7121にて発行されたものであるか否か）を判断するための認証情報で、これと同一の認証情報は、再生装置7121の第2の復号部7101dに予め格納されていて、ポイント情報に含まれている認証情報Apと照合を行うようになっている。

【0645】なお、ライセンス情報、ポイント情報の表記で用いた記号「+」は、情報がマージされることを示している。マージの際は、単にビット列を繋ぐだけでな



く、予め定められた適当な方法でビット攪乱を施しても良い。

【0646】暗号化鍵Ksは、図150のセンター装置7121が保持し、暗号化鍵Ksに対応する復号化鍵kpは、再生装置7101（図152の鍵格納部7101c）が保持している。

【0647】第3の復号部7101iに格納されているマスターキーKM、鍵格納部7101cに格納されている復号化鍵kp、第2の復号部7101dに格納されている認証情報Apは、当該レンタルサービスの加入時に各会員に渡される会員カード7102に予め記憶され、当該会員カード7102を当該会員の利用する再生装置に挿入されたときに読み取り、第3の復号部7101i、鍵格納部7101c、第2の復号部7101dに格納するようになっていてもよい。なお、再生装置7101によりマスターキーKM、復号化鍵kp、認証情報Apが読み取られた後は、会員カード7102に記録されているマスターキーKM、復号化鍵kp、認証情報Apは消去されることが望ましい。

【0648】会員カード7102に記録されているライセンス情報を用いる場合、再生装置7101でライセンス情報に含まれる利用条件等に基づき当該ライセンスが有効であると判断されると、レンタルキーKRを得ることができるので、このレンタルキーKRを用いて〔〔KD〕KM〕KRを復号し、〔KD〕KMを得る。さらに、第3の復号部7101iに格納されているマスターキーKMを用いてディスクキーKDを得る。このディスクキーKDを用いて〔KT〕KDを復号し、タイトルキーKTを得ることができる。

【0649】会員カード7102に記録されているポイント情報を用いる場合、再生装置7101でポイント情報に含まれる〔ポイント+Ap〕Ktを当該再生装置7101で発生し、一時鍵格納部7101eに予め格納されている暗号鍵Ktにて復号し、ポイントと認証情報Apを得る。認証情報Apの照合とポイントの減算処理を行った後、復号用ライセンスキーKLS(j)を用いて〔KR〕KLP(j)を復号し、レンタルキーKRを得る。以後の処理は、ライセンス情報を用いた場合と同様である。

#### (1) 再生装置

図152は、再生装置7101の構成例を示したもので、会員カード7102が挿入されて会員カード7102から各種情報データを読み取り、また、各種情報データを書き込むカード入出力部7101a、ポイント情報やライセンス情報を鍵格納部7101cに格納されている復号化鍵kpを用いて復号する第1の復号部7101b、暗号鍵Ktを発生する一時鍵発生部7101f、一時鍵発生部7101fで発生した暗号鍵Ktを一時格納する一時鍵格納部7101e、ポイント情報に含まれている〔ポイント+Ap〕Ktを一時鍵格納部7101e

に一時格納されている暗号鍵Ktを用いて復号し、認証情報Apを照合する第2の復号部7101d、ポイントを格納するポイント格納部7101g、ライセンス情報に基づきそのライセンスの有効性を判定し、当該ライセンスが有効と判定されたときレンタルキーKRを第3の復号部7101iへ出力する判定部7101h、コンテンツ情報の利用に応じてポイント格納部7101gに格納されているポイントの減算処理を行うポイント判定部7101j、メディア読取部7101mでディスク7103から読み取られた情報と判定部7101hあるいはポイント判定部7101jから送られてきた情報とに基づきコンテンツ情報を復号する第3の復号部7101i、第3の復号部7101iで復号されたコンテンツ情報を表示する表示部7101k、ポイントの利用の可否等の各種メッセージの提示やユーザからの指示入力を受け付けるためのユーザインタフェース7101lから構成されている。

【0650】次に、図153に示すフローチャートを参照して図152の再生装置7101の処理動作の概略を説明する。

【0651】入会時には会員カード7102には暗号化ライセンス情報〔〔CP〕Ks〕のみが記録されており、2回目以降のレンタル時には、暗号化ライセンス情報および暗号化ポイント情報〔〔CP〕Ks〕のうちの少なくとも1つが記録されている。

【0652】ユーザは、会員カード7102を再生装置7101に挿入すると、カード入出力部7101aは、当該会員カード7102から暗号化ポイント情報〔〔CP〕Ks〕の読み出しを行う（ステップS7101）。

【0653】暗号化ポイント情報の読み出しに成功すると（ステップS7102）、当該再生装置7101のポイント格納部7101gに既に格納されているポイントに会員カード7102から読み出されたポイント情報に含まれるポイントを加算するポイント加算処理を実行する（ステップS7103）。

【0654】次に、カード入出力部7101aは、当該会員カード7102から暗号化ライセンス情報〔〔CL〕Ks〕の読み出しを行う（ステップS7104）。

【0655】暗号化ライセンス情報の読み出しに成功すると（ステップS7105）、当該ライセンス情報に基づくライセンス判定処理を実行する（ステップS7106）。ライセンス判定処理では、ライセンス情報に基づくライセンス判定とコンテンツ情報の復号、再生を行う。一方、暗号化ライセンス情報が読み出せなかったとき（会員カード7102に暗号化ライセンス情報が記録されていないとき）は、ポイント格納部7101gに既に格納されているポイントを用いたコンテンツ情報利用に対する課金処理（ポイントの減算）、およびコンテンツ情報の復号、再生を行う（ステップS7107）。

【0656】最後に、一時鍵発生部7101fは、暗号

化鍵k tを新たに発生し、一時鍵格納部7101eに格納し、会員カード7102に記録する等のK tの更新処理を実行する(ステップS7108)。ステップS7108のK tの更新処理は、図153に示した処理動作を行う度に、すなわち、コンテンツの再生を行う度に実行される。

【0657】以上の処理動作では、会員カード7102に暗号化ライセンス情報が記録されている場合には、ライセンス情報を優先して用いている(ステップS7105)。また、会員カード7102に暗号化ポイント情報が記録されている場合、その暗号化ポイント情報が記録されてから最初に読み出した正当な再生装置(暗号化ポイント情報の復号に必要な暗号鍵k tの発生元の再生装置)のみにしか、当該ポイントは利用できないようになっている。すなわち、ステップS7108のK t更新処理では、会員カード7102に記録された暗号鍵K tを用いて暗号化ポイント情報が作成され、会員カード7102に記録されている。従って、ポイント利用範囲を当該暗号鍵k tを発生した再生装置のみに限定することができたわけである。

【0658】なお、第3の復号部7101iに格納されているマスターキーKM、鍵格納部7101cに格納されている復号化鍵K p、第2の復号部7101dに格納されている認証情報A pを更新する際には、ユーザが店舗に赴きディスクのレンタルを行った際に、更新情報をそのまま、あるいは、所定の暗号鍵で暗号化して会員カード7102に記録しておく。当該会員カード7102をユーザが再生装置に挿入した際に、再生装置7101は図153に示したような処理動作を実行する前に、会員カード7102から当該更新情報を読み出して、所定の更新処理を実行するようにしてもよい。

【0659】次に、図154に示すフローチャートを参照して図153のステップS7103におけるポイント加算処理についてより詳細に説明する。

【0660】ステップS7101で、カード入出力部7101aにて会員カード7102から読み取られた暗号化ポイント情報([CP]K s)は、第1の復号部7101bに転送される。第1の復号部7101bは、鍵格納部7101cに予め格納されている復号化鍵K pを用いてポイント情報を復号する(ステップS7111)。復号されたポイント情報に含まれる情報データのうち、[ポイント+A p]K tを第2の復号部7101dに転送する。

【0661】第2の復号部7101dでは、一時鍵格納部7101eに格納されている暗号鍵K tを用いて、[ポイント+A p]K tを復号し、ポイントと認証情報A pとを得る(ステップS7112)。そして、このポイント情報に含まれていた認証情報A pと第2の復号部7101bに既に格納されていた認証情報A pとを照合し、一致していたら、第2の復号部7101dはポイン

ト格納部7101gからそこに既に格納されているポイントを読み出して、それに、ポイント情報に含まれていたポイントを加算し、加算結果を再び、ポイント格納部7101gに格納する(ステップS7113～ステップS7116)。

【0662】ここで、K tは、図153の処理動作を実行する度に更新されるとする。この場合、会員カード7102に記録された暗号化ポイント情報は、一度、図153に示したように再生装置7101に読み出された後は、ステップS7108にてK tが更新されるので、2度目に会員カード7102に記録された暗号化ポイント情報を読み出した際には、当該暗号化ポイント情報を作成する際に用いられたK tと再生装置7101にて保持されているK tとは異なるので、正常に[ポイント+A p]K tを復号することができない。すなわち、ステップS7113において、当該ポイント情報に含まれていた認証情報A pと第2の復号部7101bに既に格納されていた認証情報A pとは不一致となるので、この場合は、ポイント加算処理を中止して、図153のステップS7104の処理に移る。

【0663】次に、図155に示すフローチャートを参照して、図153のステップS7106におけるライセンス判定処理について説明する。

【0664】ステップS7104で、カード入出力部7101aにて会員カード7102から読み取られた暗号化ライセンス情報([CL]K s)は、第1の復号部7101bに転送される。第1の復号部7101bは、鍵格納部7101cに予め格納されている復号化鍵K pを用いてライセンス情報を復号する(ステップS7121)。復号されたライセンス情報は判定部7101hへ転送され、ここで、ライセンス情報に含まれる利用条件等に基づき、前述の実施形態で説明したような当該ライセンスの有効性を判定する(ステップS7122)。

【0665】当該ライセンスが有効と判定されたとき、判定部7101hは当該ライセンス情報に含まれているレンタルキーKRを第3の復号部7101iへ転送する(ステップS7124)。

【0666】第3の復号部7101iは、レンタルキーKRと、メディア読取部7101mにてディスク7103から読み取られた情報データ([コンテンツ情報]KT、[KT]KD、[[KD]KM]KR)とを用いてコンテンツ情報を復号する。すなわち、レンタルキーKRを用いて[[KD]KM]KRを復号し、[KD]KMを得る。さらに、第3の復号部7101iに格納されているマスターキーKMを用いてディスクキーKDを得る。このディスクキーKDを用いて[KT]KDを復号し、タイトルキーKTを得ることができる。このタイトルキーKTを用いてコンテンツ情報を復号し、表示部7101kに再生表示する(ステップS7125)。

【0667】一方、ステップS7123で、当該ライセンスが無効（例えば、有効期限切れ）と判定されたときは、カード入出力部7101aは、会員カード7102から暗号化ライセンス情報を消去し（ステップS7126）、ステップS7107と同様なポイント減算処理を実行する（ステップS7127）。

【0668】次に、図156に示すフローチャートを参照して図153のステップS7107および図155のステップS7127におけるポイント減算処理について詳細に説明する。

【0669】図154のステップS7111において、第1の復号部7101bで復号されたポイント情報に含まれていた復号用ライセンスキーKLS(j)と、その識別子jは、ポイント判定部7101jに転送される（ステップS7131）。なお、課金カード7102に記録された当該暗号化ポイント情報の2度目以降の読み込みの際には、前述したように、当該暗号化ポイント情報を作成する際に用いた暗号鍵Ktと、再生装置7101の一時鍵格納部7101eに格納されている暗号鍵Ktとは異なる為、図154のステップS7112以降の処理は、常にステップS7113にて終了することとなる。従って、ポイント情報を用いコンテンツ復号動作は、図154のステップS7111から図156のポイント減算処理へ進むこととなる。

【0670】ポイント判定部7101jは、ポイント格納部7101gからポイントを読み出し、当該コンテンツ情報の利用に応じたポイント値（例えば「1」）を減算する。なお、コンテンツ情報の1回の利用（再生）に対し予め定められたポイント値（例えば「1」）を交換する場合に限らず、例えば、ディスク7102に当該ディスク7102に記録されているコンテンツ情報の利用に対し差し引くべきポイント値が予め記録されており、これを読み出して、ポイントの減算処理を行うようにしてもよい。あるいは、コンテンツ情報の制作年月日が古いものほど差し引くべきポイントの値を小さくするようにしてもよい。この場合、図152のポイント判定部7101jは、制作年月日からの経過日数に応じて予め定められた差し引くべきポイント値のリストを保持していて、ディスク7102に記録された当該コンテンツ情報の制作年月日を読み取り、当該リストを参照して、差し引くべきポイント値を決定する。ポイント判定部7101jが保持するリストは、会員カード7102（あるいは、再生装置7101がセンター装置7121とオンライン接続されている場合には通信回線）を経由して更新される。

【0671】さて、ステップS7133で得られたポイントの減算結果は負であったときは、そのまま処理動作を中断する（コンテンツ情報の再生は行わない）。

【0672】減算結果が正であるときは、ユーザインタフェース70011にポイントの利用の有無を尋ねるメ

ッセージを表示することが望ましい（ステップS7135）。このメッセージを見たユーザによりポイントの利用が指示されたときは（ステップS7136）、減算結果をポイント格納部7101gに格納する（ステップS7137）。すなわち、ポイント値を更新する。さらに、ポイント判定部7101gは、復号用ライセンスキーKLS(j)と、その識別子jとを第3の復号部7101iに転送する（ステップS7138）。

【0673】一方、メディア読取部7101mは、ディスク7103から情報データ（[KR]KLP(j)（j=1、2、3、…））を読み取り、第3の復号部7101iに転送する（ステップS7139）。

【0674】第3の復号部7101iは、識別子jに対応する暗号用ライセンスキーKLP(j)で暗号化されたレンタルキーKR、すなわち、[KR]KLP(j)を選択して、それをポイント情報に含まれていた復号用ライセンスキーKLS(j)を用いて復号し、レンタルキーKRを得る（ステップS7140）。

【0675】メディア読取部7101mは、ディスク7103から情報データ（[コンテンツ情報]KT、[KT]KD、[[KD]KM]KR）を読み取り、第3の復号部7101iに転送する。第3の復号部7101iは、レンタルキーKRを用いて[[KD]KM]KRを復号し、[KD]KMを得る。さらに、第3の復号部7101iに格納されているマスターキーKMを用いてディスクキーKDを得る。このディスクキーKDを用いて[KT]KDを復号し、タイトルキーKTを得ることができる。このタイトルキーKTを用いてコンテンツ情報を復号し、表示部7101kに再生表示する（ステップS7141）。

【0676】次に、図157に示すフローチャートを参照して図155のステップS7125および図156のステップS7141におけるコンテンツ表示処理について詳細に説明する。

【0677】メディア読取部7101mは、ディスク7103から情報データ（[KT]KD、[[KD]KM]KR）を読み取り、第3の復号部7101iに転送する（ステップS7151）。第3の復号部7101iは、レンタルキーKRを用いて[[KD]KM]KRを復号し、[KD]KMを得る。さらに、第3の復号部7101iに格納されているマスターキーKMを用いてディスクキーKDを得る。このディスクキーKDを用いて[KT]KDを復号し、タイトルキーKTを得ることができる（ステップS7152）。

【0678】メディア読取部7101mは、ディスク7103から暗号化コンテンツ情報[コンテンツ情報]KTを読み取り、第3の復号部7101iに転送する（ステップS7153）。第3の復号部7101iは、タイトルキーKTを用いてコンテンツ情報を復号し（ステップS7154）、表示部7101kに再生表示する（ス

テップS7155)。

【0679】次に、図153のステップS7108の暗号鍵Ktの更新処理について、図158に示すフローチャートを参照して説明する。

【0680】例えば、ポイント情報あるいはライセンス情報を用いたコンテンツの表示処理が終了した後、図155のステップS7123でライセンスが無効と判断されたとき、図156のステップS7134でポイントの使いきりが検知されたとき、一時鍵生成部7101fは、暗号鍵ktを生成する(ステップS7161)。なお、暗号鍵生成方法は、ここでは、特に限定しない。

【0681】一時鍵発生部7101fで生成された暗号鍵Ktは一時鍵格納部7101eに格納され(ステップS7162)、さらにカード入出力部7101aから会員カード7102に当該更新された暗号鍵Ktが書き込まれる(ステップS7163)。

#### (2) ライセンス/ポイント注入装置

図159は、ライセンス/ポイント注入装置7111の構成例を示したもので、センター装置7121に接続して、ライセンス情報/ポイント情報の発行要求を送信したり、当該要求に応じてセンター装置7121から発行されライセンス情報/ポイント情報を受信するための通信部7111a、会員カード7102が挿入されて会員カード7102から各種情報データを読み取り、また、各種情報データを書き込むカード入出力部7111c、ディスク7103から各種情報データを読み出すためのメディア読取部7111e、ライセンス情報にマージされる利用条件や、ポイント情報にマージされるポイント等の情報データを入力するための条件入力部7111d、上記各部を制御する制御部7111bから構成されている。

【0682】次に、図160、図161に示すフローチャートを参照して図159のライセンス/ポイント注入装置7111の処理動作の概略を説明する。

【0683】まず、図160を参照して、ライセンス情報発行処理動作について説明する。例えば店舗の店員が当該レンタルサービスの会員の会員カード7102をカード入出力部7111cに挿入し、当該会員により選択されたディスク7103をメディア読取部7111eにセットする。店員は、条件入力部7111dから当該ディスク7103に記録されているコンテンツ情報に対する利用条件等を入力し、ライセンス情報発行要求の指示入力を行うと(ステップS7171)、メディア読取部7111eは、ディスク7103からコンテンツIDを読み取る(ステップS7172)。制御部7111bは、通信部7111aを介してセンター装置7121へ、コンテンツの利用条件、コンテンツIDを含むライセンス情報の発行要求を送信する(ステップS7173)。

【0684】ライセンス情報の発行要求を受けてセンタ

ー装置7121にて発行された暗号化ライセンス情報([CL]Ks)は、通信部7111aで受信される(ステップS7174)。制御部7111bは、通信部7111aで受信された暗号化ライセンス情報をカード入出力部7111cへ転送し、カード入出力部7111cは、当該暗号化ライセンス情報を会員カード7102に記録する(ステップS7175)。

【0685】次に、図161を参照して、ポイント情報発行処理動作について説明する。

【0686】例えば店舗の店員が当該レンタルサービスの会員の会員カード7102をカード入出力部7111cに挿入する。店員は、条件入力部7111dから購入されたポイントを入力し、ポイント情報発行要求の指示入力を行うと(ステップS7181)、カード入出力部7111cは、会員カード7102から暗号化ポイント情報を読み取る(ステップS7182)。ここで、読み取られた暗号化ポイント情報は、消去してもよい。

【0687】次に、カード入出力部7111cは会員カード7102から暗号鍵Ktを読み取る(ステップS7183)。暗号鍵Ktを読み取ることができなかったときは、ポイント情報の発行ができないので、処理を中断する。

【0688】一方、暗号鍵Ktの読み取りに成功した場合は(ステップS7184)、制御部7111bは、通信部7111aを介してセンター装置7121へポイント値、暗号鍵Ktを含むポイント情報の発行要求を送信する(ステップS7185)。

【0689】ポイント情報の発行要求を受けてセンター装置7121にて発行された暗号化ポイント情報([CP]Ks)は、通信部7111aで受信される(ステップS7186)。制御部7111bは、通信部7111aで受信された暗号化ポイント情報をカード入出力部7111cへ転送し、カード入出力部7111cは、当該暗号化ポイント情報を会員カード7102に記録する(ステップS7187)。

#### (3) センター装置

図162は、センター装置7121の構成例を示したもので、第1の暗号化部7121a、第2の暗号化部7121b、鍵格納部7121c、認証情報格納部7121d、ライセンスキー格納部7121e、通信部7121f、コンテンツデータベース7021g、時計7021hから構成されている。

【0690】コンテンツデータベース7021gには、コンテンツIDに対応させて、レンタルキーKRが記憶されている。

【0691】鍵格納部7121cには、ライセンス情報とポイント情報を暗号化するための暗号鍵Ksが格納されている。

【0692】認証情報格納部7121dには、認証情報Apが格納されている。

【0693】ライセンスキー格納部7121eには、復号用ライセンスキーKLS(j) (j=1、2、3、…)が格納されている。

【0694】通信部7121fは、ライセンス/ポイント注入装置7111に接続して、ライセンス情報/ポイント情報の発行要求を受信したり、当該要求に応じて発行したライセンス情報/ポイント情報をライセンス/ポイント注入装置7111に送信する。

【0695】次に、図163、図164に示すフローチャートを参照して図162のセンター装置7121の処理動作の概略を説明する。

【0696】まず、図163を参照して、ライセンス情報発行処理動作について説明する。通信部7121fは、ライセンス/ポイント注入装置7111から、コンテンツの利用条件、コンテンツIDを含むライセンス情報の発行要求を受信すると(ステップS7191)、第1の暗号化部7121aへコンテンツIDと利用条件等を転送する(ステップS7192)。

【0697】第1の暗号化部7121aは、コンテンツデータベース7021gから当該コンテンツIDに対応するレンタルキーKRを読み出し(ステップS7193)、時計7021hから現在日時を読み出し(ステップS7194)、さらに、鍵格納部7121cから暗号鍵Ksを読み出し、暗号化ライセンス情報[CL]Ks=[KR+ライセンス情報作成日時+利用条件]Ksを作成する(ステップS7195)。

【0698】通信部7121fは、第1の暗号化部7121aで作成された暗号化ライセンス情報をライセンス/ポイント注入装置7111へ送信する(ステップS7196)。

【0699】図164に示すフローチャートを参照して、ポイント情報発行処理動作について説明する。

【0700】通信部7121fは、ライセンス/ポイント注入装置7111から、ポイント値と暗号鍵Ktを含むポイント情報の発行要求を受信すると(ステップS7201)、第2の暗号化部7121bへポイント値と暗号鍵Ktとを転送する(ステップS7202)。

【0701】第2の暗号化部7121bは、認証情報格納部7121dから認証情報Apを読み出し(ステップS7203)、当該認証情報とポイント情報とをマージして、さらに暗号鍵Ktで暗号化し、[ポイント情報+Ap]Ktを生成する(ステップS7204)。

【0702】第1の暗号化部7121aは、ライセンスキー格納部7121eから復号用ライセンスキーKLS(j)とその識別子jを1組読み出し(ステップS7205)、[ポイント情報+Ap]Ktと復号用ライセンスキーKLS(j)とその識別子jとをマージして、さらに、鍵格納部7121cから読み出された暗号鍵Ksで暗号化して、暗号化ポイント情報[CP]Ks=[ポイント情報+Ap]Kt+復号用ライセンスキー

KLS(j)+j]Ksを作成する(ステップS7206)。

【0703】通信部7121fは、第1の暗号化部7121aで作成された暗号化ポイント情報をライセンス/ポイント注入装置7111へ送信する(ステップS7207)。

【0704】なお、上記実施形態において、再生装置7101の購入時(当該レンタルサービス入会時)に、例えば店舗にて、あるいは、再生装置7101の製造時に、第3の復号部7101i、鍵格納部7101c、第2の復号部7101dにそれぞれ、マスターキーKM、復号化鍵Kp、認証情報Apを書き込むようにしてもよい。

【0705】また、例えば、当該レンタルサービス入会時に購入した再生装置7101にはそれに対応した会員カード7102が添付されており、この会員カード7102には、既に再生装置7101にて発生された暗号鍵Ktが書き込まれているものであってもよい。この場合、上記実施形態では、初回目は必ずライセンス情報を用いなければならなかったが、レンタルサービス入会時には、既に会員カード7102に再生装置7101にて発生された暗号鍵Ktが書き込まれているので、当該レンタルサービス入会と同時にポイント情報を用いたコンテンツ再生が行えるようになる。

【0706】また、上記実施形態では、会員の利用する再生装置7101から発生される暗号鍵Ktを用いて暗号化ポイント情報を作成することにより、当該会員により購入されたポイントの使用を当該会員の使用する再生装置7101のみに限定するものであったが、この場合に限らず、さらに、当該ポイントの利用を特定のコンテンツ(あるいは特定のカテゴリーのコンテンツ)に限定することも可能である(例えば、未成年者には視聴可能なカテゴリーを限定することができる)。この場合、例えば、暗号用ライセンスキーKLP(1)、KLP(2)、KLP(3)、…を用いることにより、レンタル業者側から(必要があれば、会員に知られることなく)操作することができる。すなわち、例えば、会員により購入されたポイントの利用を特定のカテゴリーに属するコンテンツの再生のみに限定する場合には、当該購入されたポイントを含む暗号化ポイント情報には、複数の復号用ライセンスキーのうち、当該限定したいカテゴリーに対し予め割り当てられた復号用ライセンスキーKLS(j)のみが含まれていればよい。もちろん、ディスク7103には、そこに記録されているコンテンツのカテゴリーに応じた暗号用ライセンスキーKLP(j)で暗号化されたレンタルキーKRのみが記録されている。

【0707】以上説明したように、上記実施形態によれば、

- ・ 会員が利用する再生装置で発生された各再生装置固

有の暗号鍵Ktを用いて暗号化ポイント情報を作成することにより、当該会員により購入されたポイントの利用を当該会員の利用する再生装置にのみに限定することができる。

【0708】コンテンツのカテゴリ毎にライセンスキー(KLP(j)とKLS(j))を定め、暗号化ポイント情報に当該会員に視聴可能なカテゴリの復号用ライセンスキーKLS(j)のみが含まれていることにより、また、貸し出されるディスクには、そこに記録されているコンテンツのカテゴリに応じた暗号用ライセンスキーKLP(j)で暗号化されたレンタルキーKRのみが記録されていることにより、会員により購入されたポイントの利用を、当該会員が視聴可能なカテゴリのコンテンツの視聴にのみに限定することができる。

(4) ポイントのみを用いたレンタルサービスの実施形態

以下、競合する複数のレンタル業者により提供される複数のレンタルサービスに1つの再生装置を用いる場合を例にとり説明する。

【0709】上記した実施形態では、初回目は必ずライセンス情報を用いなければならなかったが、レンタルサービス入会時から、すなわち、初回目からライセンス情報を用いることなく、ポイントのみを用いたレンタルサービスを実現する方が再生装置の構成を簡略化する上で有効である(例えば、判定部7101でライセンス情報に含まれる利用条件(例えば期限)の有効性を判定するために必要な時計が不要となる)。

【0710】そこで、入会直後の初回目のレンタル時に会員カード7102に書き込まれる初回暗号化ポイント情報[CP0]Ksの構成を初回暗号化ポイント情報([CP0]Ks)=[ポイント+j+KLS(j)+業者ID]Ksとする。

【0711】業者IDとは、異なるレンタル業者のそれぞれを識別するためのIDであるとともに、ポイント格納部7101gへのポイント値の書込および読み出しを制御するために用いる情報である。

【0712】また、ポイント格納部7101gには、レンタル業者毎に業者IDとそのポイント値を書き込む領域がそれぞれ設けられている。

【0713】また、2回目以降にポイントを購入した際に作成される暗号化ポイント情報には、さらに業者IDが含まれている。すなわち、ここで用いる暗号化ポイント情報[CP]Ks'は、

暗号化ポイント情報([CP]Ks')=[ポイント+Ap]Kt+j+KLS(j)+業者ID]Ksと表すことができる。

【0714】以下、再生装置7101の初回暗号化ポイント情報の処理動作について説明する。

【0715】ステップS7301) 図153のステップS7101にて再生装置7101が会員カード710

2から通常の暗号化ポイント情報([CP]Ks')を読み出す前に、上記初回暗号化ポイント情報[CP0]Ksの読み出しを行う(会員カード7102には、[CP]Ks'と[CP0]Ksの両方が書き込まれていてもよい)。

【0716】ステップS7302) カード入出力部7101aで読み出された初回暗号化ポイント情報は、第1の復号部7101bへ転送され、第1の復号部7101bにて復号化鍵Kpを用いて初回ポイント情報を復号し、その中に含まれている業者ID(例えば「xx」とする)と、ポイントを判定部7101hへ転送する。判定部7101hは、ポイント格納部7101gから当該業者ID(xx)を検索し、ポイント格納部7101gに当該業者ID(xx)が未だ書き込まれていないときのみ、当該ポイント値を当該業者ID(xx)に対応させてポイント格納部7101gに書き込む。

【0717】当該同一業者の初回暗号化ポイント情報を用いた2回目以降のコンテンツ再生時には、再び、上記処理(ステップS7301～ステップS7302)を実行することになるが、その場合には、ポイント格納部7101gに当該業者ID(xx)が既に書き込まれているので、再び、同じ初回暗号化ポイント情報によるポイントの書き込み(加算)は行うことなく、図153のステップS7101の処理に進む。

【0718】一方、ステップS7301にて異なる業者(業者ID(yy))の初回暗号化ポイント情報を新たに読み出した場合、ポイント格納部7101gに、その業者IDが存在しない限り、当該業者ID(yy)と、当該初回暗号化ポイント情報に含まれていたポイント値とをポイント格納部7101gに書き込む。

【0719】以上の処理動作が、図153のステップS7101の前段に追加され、以後の処理動作は、前述同様である。すなわち、2回目以降のポイント購入時には、当該再生装置7101が発生した暗号鍵Ktを用いて暗号化ポイント情報([CP]Ks')が作成される。

【0720】異なるのは、2回目以降のポイントの購入時に作成される暗号化ポイント情報には前述したように、そのポイントを購入したレンタル業者のIDが含まれていて、図153～図158に示したような処理動作は、この業者IDに対応してポイント格納部7101gに記録されたポイントが減算されることにより実行されることである。より詳しくは、図153のステップS7101～ステップS7103、ステップS7107～ステップS7108に対応する処理動作のみを行うことになる。

【0721】暗号化ポイント情報[CP]Ks'に含まれる業者IDの確認は、判定部7101hにて行うものとする。すなわち、図154のステップS7111において、暗号化ポイント情報[CP]Ks'を復号する

と、その中に含まれていた業者IDは判定部7101hに転送され、ステップS7116において、第2の復号部7101dがポイント格納部7101gにポイント値を書き込む際には、判定部7101hにて指示された業者IDに対応するポイント書込領域に書き込む。また、図156のポイント減算処理のステップS7132、ステップS7137において、ポイント判定部7101jがポイント格納部7101gからポイントを読み書きする際には、判定部7101hにて指示された業者IDに対応するポイント書込領域から当該ポイント値の読み出し/書き込みを行う。

【0722】なお、レンタル業者が1つのみの場合も上記同様である。すなわち、業者IDが1つのみしかこの世に存在しない場合も、入会直後からポイントを用いたレンタルサービスが実現できる。この場合、業者IDとは、単に、初回にポイント格納部7101gへポイント値の書き込みを制御するために用いるだけである。

【0723】以上説明したように、暗号化ポイント情報は業者IDを含み、初回のみ、業者IDを用いてポイント格納部7101gへのポイント値の書き込みを制御することにより、ポイントのみを用いたレンタルサービスが容易に行える。

【0724】また、ポイント格納部7101gには、業者ID毎にポイント書込領域が設けられていて、暗号化ポイント情報に含まれている業者IDに基づき、ポイント格納部7101gに格納されているポイントを減算することにより、1つの再生装置で複数の競合するレンタル業者のそれぞれにて販売されるポイントを利用することができる。この場合、貸し出されるディスクは複数のレンタル業者で共通したものであってもよいし、レンタル業者毎に異なってもよい。

(第7の実施形態)

(7-1) 図165は、本発明の第7の実施形態に係る情報流通システムに用いられる再生装置の構成例を示したもので、DVD、CD、LD、ビデオテープ等の記録メディア(以下、簡単にメディアと呼ぶ)8001からメディア記録情報を読み出すメディア読取部8102と、復号ユニット8103と、表示装置8112とから構成されている。

【0725】メディア読取部8102は、メディア8101に対応した従来からある読取装置(例えばメディア8101がDVDならばDVDプレーヤ、CDならCDプレーヤ)を用いる。

【0726】ここでは、メディア8103に記録されている暗号化コンテンツ情報の利用に対する点数(ポイント)を予め購入して、メディア8103を貸し出すことによりなるレンタルサービスを提供するための再生装置について説明する。

【0727】メディア8101には、図166に示すように、コンテンツキーKcで暗号化された課金対象のコ

ンテンツ情報(暗号化コンテンツ情報)に、当該コンテンツキーKcをレンタルキーKrで暗号化して生成したWM情報を電子すかし(Digital Watermark)技術で合成して得られるメディア記録情報が記録されている。

【0728】ここで、「コンテンツ情報を暗号化する」とは、例えばコンテンツ情報が画像であれば、その輝度を変えるとといった、当該コンテンツ情報に対しその実体が視聴者には明らかにならないように施す加工処理を含むものである。従って、ここで、コンテンツキーKcとは、この加工処理を施されたコンテンツを復元するために必要な情報である。

【0729】コンテンツキーKcは、コンテンツ情報の暗号化復号化鍵で、少なくともコンテンツのタイトル毎に異なっていることが望ましい。

【0730】レンタルキーKrは、コンテンツキーの暗号化復号化鍵で、例えば、同時期に製造されたディスク7103には同一のレンタルキーが用いられる。

【0731】WM情報の埋め込み位置としては、暗号化コンテンツ情報の全体に均一に、あるいは所定間隔毎に埋め込むようにしてもよし、図172に示すように、コンテンツ情報の先頭にある未暗号化部分に埋め込むようにしてもよい。この場合、コンテンツ情報に、WM情報が埋め込まれてなく、かつ、暗号化されていない領域(例えば、WN情報の処理時間相当分)R100が存在していてもよい。なお、暗号化されていない領域R100は、WM情報の埋め込み領域の前方にあってもよい。いずれにしても、当該WM情報の埋め込み位置は、暗号化コンテンツ情報の前方にあるべきである。

【0732】コンテンツ情報の利用に対する予め購入されたポイントは、カード型記録媒体(以下、カードと呼ぶ)8010に記録されていて、カード8110は復号ユニット8103に挿入することにより、メディア8101に記録されているコンテンツ情報の再生が行えるようになっている。すなわち、メディア8101に記録されているコンテンツ情報を再生する度に当該コンテンツ情報に応じて所定値のポイントがカード8110に予め記録されているポイントが減算されていく。このポイント値がなくなると、コンテンツ情報の再生は行えない。

【0733】カード8110には、少なくとも、支払った金額に応じたポイント値と、レンタルキーKrとが記録されている。ポイント値とレンタルキーKrはそのまま記録されていてもよいが、所定の加工処理(例えば、暗号化処理等)を施してから記録するようにしてもよい。

【0734】レンタルキーKrは、レンタル時、あるいは、ポイント購入時にカード8110に記録されるものとしてもよい。

【0735】以下、図167に示すフローチャートを参照して、図165の再生装置の処理動作について説明す

る。

【0736】メディア読取部8102にメディア8101がセットされ、復号ユニット8103にカード8110が挿入されると、メディア8101に記録されたメディア記録情報(C')は、メディア8101に対応した読取装置(例えばメディア8101がDVDならばDVDプレーヤ、CDならCDプレーヤ)で読み取られ、復号ユニット8103へ出力される。メディア記録情報(C')は、復号ユニット8103のWM分離部8104に入力する(ステップS8101)。

【0737】WM分離部8104は、入力したメディア記録情報(C')を暗号化コンテンツ情報(C'')とWM情報(W)とに分離し、前者をコンテンツ復号部8108に、後者をWM格納部8105にそれぞれ転送する(ステップS8102、ステップS8103)。

【0738】一方、ポイント減算部8109は、挿入されたカード8110からポイントを読み出し、当該ポイント値がこれから再生しようとするコンテンツ情報の利用に対するポイント値以上の値であるか(有効量であるか)否かを判断する。当該ポイント値が有効量(例えば、ポイント>0)である判断すると、キー復号部8106を起動する。起動されたキー復号部8106は、WM格納部8105からWM情報を読み出す。さらに、ポイント減算部8109は、カード8110からレンタルキーKrを取得し、キー復号部8106へ転送する(ステップS8104～ステップS8106)。キー復号部8106は、レンタルキーKrを用いてWM情報からコンテンツキーKcを復号し、キー格納部5007に格納する(ステップS8106～ステップS8107)。

【0739】一方、コンテンツ復号部5008は、WM分離部5004から渡された暗号化コンテンツ情報(C'')をキー格納部5007から読み出したコンテンツキーKcで復号してコンテンツ情報(C)を得、表示装置5011へ出力する(ステップS8109～ステップS8110)。

【0740】ステップS8105で、カード8110のポイント値が有効量でないと判断されたとき、もしくは、ステップS8106でカード8110から出力されたレンタルキーがWM情報生成に用いたレンタルキーKrと相違していたときは、コンテンツ情報は正常に復号されず、利用者に提示されないことになる。

(7-2) 図168は、第7の実施形態に係る情報流通システムに用いられる再生装置の他の構成例を示したものである。なお、図165と同一部分には同一符号を付し、異なる部分についての説明を省略する。すなわち、図165のメディア読取部8102が図168では、放送波受信部(チューナ)8021に置き換わっていて、図166に示したようなメディア記録情報が放送波として各ユーザ宅に配信されるようになっている。チューナ8021は、受信した放送波から抽出されたメディア記録情

報(C')を復号ユニット8103へ出力する。

(7-3) メディア記録情報の他の例を図170を参照して説明する。図166に示したメディア記録情報と異なるのは、WM情報である。すなわち、図170では、1つのコンテンツキーKcを複数のレンタルキーKr1、Kr2、…、Krnで暗号化したものを結合(マージ)し、それをWM情報としている。

【0741】図170に示したようなメディア記録情報を用いた再生装置の構成例を図169に示す。なお、図169において、図165と同一部分には同一符号を付し、異なる部分についての説明を省略する。すなわち、カード8130には、複数のレンタルキーKr1、Kr2、…、Krnのうちの1つ、あるいは複数、あるいは全てが記録されている。

【0742】図171は、図169の再生装置の処理動作を説明するためのフローチャートである。なお、図167と同一部分には同一符号を付し、異なる部分についての説明を省略する。すなわち、図167のS8006とステップS8107が、図171ではステップS8121とステップS8122に置き換わっている。

【0743】キー復号部8131は、カード8130から出力される複数のレンタルキーのうちの1つ(Kri)を用いてWM情報からコンテンツキーKcを得るようになっている。カード8130に複数のライセンスキーが記録されている場合は、それらを1つずつ読み出して、WM情報を復号していく。

【0744】WM情報には、コンテンツキーの他に、正確に復号できたか否かをチェックするための予め決められた認証情報が含まれることが望ましい。この認証情報が正確に復号できたか否かにより、正当なコンテンツキーが得られたか否かが容易に判断できる。

【0745】ステップS8105で、カード8110のポイント値が有効量でないと判断されたとき、もしくは、ステップS8121でカード8130から出力されたレンタルキーがWM情報生成に用いたレンタルキーKr1、Kr2、…、Krnのいずれとも合致しないときは、コンテンツ情報は正常に復号されず、利用者に提示されないことになる。

【0746】

【発明の効果】以上説明したように、本発明の情報記録装置および情報再生装置および課金装置によれば、ネットワークあるいは記録媒体を介して分配されたデジタル化された著作物を迅速かつ手軽に流通させるとともに、デジタル情報の利用に対する課金による著作権の保護を前提としたデジタル情報の利用環境を容易に構築できる。

【図面の簡単な説明】

【図1】本発明の実施形態に係る情報記録装置の第1の構成例を示した図。

【図2】図1の第1の情報記録装置の動作を説明するた



めのフローチャート。

【図3】本発明の実施形態に係る情報記録装置の第2の構成例を示した図。

【図4】図3の第2の情報記録装置の動作を説明するためのフローチャート。

【図5】課金対象情報データの分離方法を説明するための図。

【図6】課金対象情報データの他の分離方法を説明するための図。

【図7】本発明の実施形態に係る情報記録装置の第3の構成例を示した図。

【図8】本発明の実施形態に係る情報再生装置の第1の構成例を示した図。

【図9】図8の復号ユニットの構成例を示した図。

【図10】図8の第1の情報再生装置の動作を説明するためのフローチャート。

【図11】図9の復号ユニットの動作を説明するためのフローチャート。

【図12】復号ユニットの他の構成例を示した図で、時刻の更新を無効にする時計を具備した復号ユニットの場合を示している。

【図13】復号ユニットに具備される時計の時刻の更新を無効にするための動作を説明するためのフローチャート。

【図14】図12の復号ユニットの動作を説明するためのフローチャート。

【図15】時刻の更新が可能な復号ユニットに具備された時計の構成例を示した図。

【図16】図15の時計の時刻更新動作を説明するためのフローチャート。

【図17】ネットワークを介して復号ユニットに具備された時計の時刻更新を行う場合のクライアントとサーバとで構成されるシステムの全体図。

【図18】図17の時刻設定クライアントの構成例を示した図。

【図19】図17の時刻設定サーバの構成例を示した図。

【図20】図18の時刻設定クライアントの動作を説明するためのフローチャート。

【図21】図19の時刻設定サーバの動作を説明するためのフローチャート。

【図22】図19の時刻設定サーバの動作を説明するためのフローチャート。

【図23】図18の時刻設定クライアントに具備される時計の構成例を示した図。

【図24】図23の時計の動作を説明するためのフローチャート。

【図25】図23の時計の動作を説明するためのフローチャート。

【図26】ライセンス情報の更新および課金を行う機能

を具備した情報再生装置（第2の情報再生装置）の構成例を示した図。

【図27】図26の復号ユニットの構成例を示した図。

【図28】図27の復号ユニットの動作を説明するためのフローチャート。

【図29】図26のライセンス情報更新クライアント部の構成例を示した図。

【図30】図29のライセンス情報更新クライアント部の動作を説明するためのフローチャート。

【図31】図26のライセンス情報更新サーバの構成例を示した図。

【図32】図31のライセンス情報更新サーバの動作を説明するためのフローチャート。

【図33】ライセンス情報更新サーバから出力される課金対象情報の利用に対する料金の支払い要求の内容の一例を示した図。

【図34】図26のシステム全体（ネットワークを介し互いに通信を行うサーバおよびクライアント）の動作を説明するためのフローチャート。

【図35】ライセンス情報更新ユニットの構成例を示した図。

【図36】図35のライセンス情報更新ユニットの動作を説明するためのフローチャート。

【図37】図35のライセンス情報更新ユニットの動作を説明するためのフローチャート。

【図38】課金対象情報の利用に対する課金を行うための課金装置の構成例を示した図。

【図39】課金対象情報の不正コピーの防止対策（復号ユニットIDに基づく判定を行う）を講じた情報再生装置の復号ユニットの構成例を示した図。

【図40】図39の動作を説明するためのフローチャート。

【図41】課金対象情報の不正コピーの防止対策を講じたライセンス情報更新ユニットの構成例を示した図。

【図42】図41のライセンス情報更新ユニットの動作を説明するためのフローチャート。

【図43】課金対象情報の不正コピーの防止対策を講じた（復号ユニットIDおよびメディアIDに基づく判定を行う）復号ユニットの他の構成例を示した図。

【図44】図43の復号ユニットの動作を説明するためのフローチャート。

【図45】コピー装置の構成例を示した図。

【図46】図45のコピー装置の動作を説明するためのフローチャート。

【図47】図45のライセンス情報複製ユニットの構成例を示した図。

【図48】図47のライセンス情報複製ユニットの動作を説明するためのフローチャート。

【図49】本発明の実施形態に係る副情報を再生する場合の情報再生装置（第3の情報再生装置）の構成例を示

した図。

【図50】図49の第3の情報再生装置の構成例を示した図。

【図51】図49の復号ユニットの構成例を示した図。

【図52】図51の復号ユニットの動作を説明するためのフローチャート。

【図53】本発明に係る情報記録装置および情報再生装置を用いた情報流通システムの構成例を示した図。

【図54】本発明の第2の実施形態に係る復号ユニットAの構成例を示した図。

【図55】復号ユニットAに入力するライセンス情報の一例を示した図。

【図56】復号ユニットAから出力する更新情報の一例を示した図。

【図57】復号ユニットAの処理動作を説明するためのフローチャート。

【図58】復号ユニットAの鍵保持部、鍵生成部における鍵生成処理の概略手順を説明するためのフローチャート。

【図59】復号ユニットBの構成例を示した図。

【図60】復号ユニットBに入力するライセンス情報の一例を示した図。

【図61】復号ユニットBの処理動作を説明するためのフローチャート。

【図62】復号ユニットBから出力する更新情報の一例を示した図。

【図63】復号ユニットCの構成例を示した図。

【図64】復号ユニットCから出力する更新情報の一例を示した図。

【図65】復号ユニットDの構成例を示した図。

【図66】復号ユニットDに入力するライセンス情報の一例を示した図。

【図67】復号ユニットDの処理動作を説明するためのフローチャート。

【図68】復号ユニットDの処理動作を説明するためのフローチャート。

【図69】復号ユニットDから出力する更新情報の一例を示した図。

【図70】復号ユニットD'の構成例を示した図。

【図71】復号ユニットAに対応するライセンス情報更新装置の構成例を示した図。

【図72】図71のライセンス情報更新装置の処理動作を説明するためのフローチャート。

【図73】復号ユニットBに対応するライセンス情報更新装置の構成例を示した図。

【図74】図73のライセンス情報更新装置の処理動作を説明するためのフローチャート。

【図75】第3の実施形態に係る情報流通システムの構成例を示した図。

【図76】第3の実施形態に係る情報流通システムの他

の構成例を示した図。

【図77】復号判定カードを装着した情報再生装置の要部の構成例を示した図。

【図78】図75の情報流通システムで用いられる図77の情報再生装置の処理動作を説明するためのフローチャート。

【図79】復号判定カードの要部の構成例を示した図。

【図80】図79の復号判定カードの処理動作を説明するためのフローチャート。

【図81】図79の復号判定カードの時刻転送部の構成例を示した図。

【図82】図81の時刻転送部の認証部の構成例を示した図。

【図83】図82の認証部の処理動作を説明するためのフローチャート。

【図84】図79の復号判定カードのコンテンツキー転送部の構成例を示した図。

【図85】図84のコンテンツキー転送部の認証部の構成例を示した図。

【図86】図85の認証部の処理動作を説明するためのフローチャート。

【図87】図77の時計の構成例を示した図。

【図88】図87の時計の認証部の構成例を示した図。

【図89】図88の認証部の処理動作を説明するためのフローチャート。

【図90】図79の復号判定部の構成例を示した図。

【図91】図90の復号判定部の処理動作を説明するためのフローチャート。

【図92】図77の情報再生部の構成例を示した図。

【図93】図92の情報再生部の処理動作を説明するためのフローチャート。

【図94】図92の情報再生部の認証部の構成例を示した図。

【図95】図94の認証部の処理動作を説明するためのフローチャート。

【図96】図77の情報再生部の他の構成例を示した図。

【図97】ライセンス更新装置の構成例を示した図。

【図98】ライセンス更新装置の処理動作を説明するためのフローチャート。

【図99】ライセンス更新装置の更新IFとのインターフェースを司る復号判定カードの要部の構成例を示した図。

【図100】ライセンス更新時の復号判定カードの処理動作を説明するためのフローチャート。

【図101】ライセンスサーバの構成例を示した図。

【図102】ライセンスサーバの処理動作を説明するためのフローチャート。

【図103】電子決済を利用してライセンスを更新する場合のユーザ端末、ライセンスサーバ、電子決済装置か

らなるシステム構成の一例を示した図。

【図104】図103のシステム構成におけるライセンス更新装置の構成例を示した図。

【図105】図103のシステム構成におけるライセンスサーバの構成例を示した図。

【図106】図103のシステム構成においてライセンス更新を行う場合のシステム全体の処理動作を説明するためのフローチャート。

【図107】本発明の第4の実施形態に係る情報再生システムの全体の構成例を示した図。

【図108】図107のライセンス判定ユニットの構成例を示した図。

【図109】図107の情報再生装置の処理動作を説明するためのフローチャート。

【図110】図107の情報再生装置の処理動作を説明するためのフローチャート。

【図111】図107の情報再生装置において、ライセンス情報をライセンスデータベースへ格納するまでの処理動作を説明するためのフローチャート。

【図112】図107の情報生成装置において、ライセンス情報の復号鍵の生成処理動作について説明するためのフローチャート。

【図113】コンテンツ情報の構成例を示した図。

【図114】ライセンス情報の構成例を示した図。

【図115】ライセンス情報データベースにおけるライセンス情報の記憶例を示した図。

【図116】ライセンス更新情報の構成例を示した図。

【図117】ライセンス情報データベースにおけるライセンス情報の他の記憶例を示した図。

【図118】図107に示した情報再生装置の他の構成例を示した図。

【図119】図107のライセンス判定ユニットの他の構成例を示した図。

【図120】図118の情報再生装置において、受信した放送波から暗号化ライセンス情報と復号鍵のシード情報を分離して復号鍵を生成するまでの動作について説明するためのフローチャート。

【図121】放送波のデータ構造の一例を示した図。

【図122】本発明の第5の実施形態に係る情報流通システムの構成例を示した図。

【図123】レンタル用のディスクに記録されているデータの一例を示した図。

【図124】センタに設けられたコンテンツデータベースにおけるディスクキーの記憶例w示した図。

【図125】図122に示した情報流通システムにおけるディスクキーの配送方式を概略的に示した図。

【図126】ライセンス作成装置の構成例を示した図。

【図127】ライセンス注入装置の構成例を示した図。

【図128】カードの構成例を示した図。

【図129】カードアダプタの構成例を示した図。

【図130】プレーヤの構成例を示した図。

【図131】ライセンス作成装置におけるディスク情報作成処理動作を説明するためのフローチャート。

【図132】ライセンス注入装置のライセンスデータベースにおけるディスク情報の記憶例を示した図。

【図133】図122の情報流通システムにおけるディスクキーの配信手順の概略をディスクレンタルサービスへの加入時、ディスクのレンタル時、コンテンツ再生時の順に示したシーケンス図。

【図134】図133に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図135】図133に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図136】図133に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図137】図133に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図138】図133に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図139】図133に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図140】図133に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図141】図122の情報流通システムにおけるディスクキーの他の配信手順の概略をディスクレンタルサービスへの加入時・ディスクのレンタル時、コンテンツ再生時の順に示したシーケンス図。

【図142】図141に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図143】図141に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図144】図141に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図145】図141に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図146】図141に示したディスクキーの配信手順をより詳細に示したフローチャート。

【図147】暗号パラメータ更新処理動作を説明するためのフローチャート。

【図148】暗号パラメータ更新処理動作を説明するためのフローチャート。

【図149】暗号パラメータ更新処理動作を説明するためのフローチャート。

【図150】本発明の第6の実施形態に係る情報流通システムの構成例を示した図。

【図151】レンタルサービス提供のために、ディスク、会員カード、再生装置のそれぞれにおいて用いられる情報データについて説明するための図。

【図152】再生装置の構成例を示した図。

【図153】図152の再生装置の処理動作の概略を説

明するためのフローチャート。

【図154】ポイント加算処理動作を説明するためのフローチャート。

【図155】ライセンス判定処理動作を説明するためのフローチャート。

【図156】ポイント減算処理動作を説明するためのフローチャート。

【図157】コンテンツ表示処理動作を説明するためのフローチャート。

【図158】暗号鍵K<sub>t</sub>の更新処理動作を説明するためのフローチャート。

【図159】ライセンス／ポイント注入装置の構成例を示した図。

【図160】ライセンス／ポイント注入装置のライセンス情報発行処理動作を説明するためのフローチャート。

【図161】ライセンス／ポイント注入装置のポイント情報発行処理動作を説明するためのフローチャート。

【図162】センター装置の構成例を示した図。

【図163】センター装置のライセンス情報発行処理動作を説明するためのフローチャート。

【図164】センター装置のポイント情報発行処理動作を説明するためのフローチャート。

【図165】本発明の第7の実施形態に係る情報流通システムに用いられる再生装置の構成例を示した図。

【図166】メディア記録情報の一例を示した図。

【図167】図165の再生装置の処理動作について説明するためのフローチャート。

【図168】再生装置の他の構成例を示した図。

【図169】再生装置のさらに他の構成例(図170のメディア記録情報を用いた場合)を示した図。

【図170】メディア記録情報の他の例を示した図。

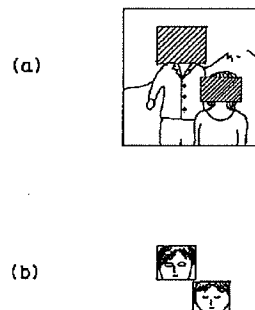
【図171】図170のメディア記録情報を用いた場合の169の再生装置の処理動作について説明するためのフローチャート。

【図172】WM情報の埋め込み位置について説明するための図。

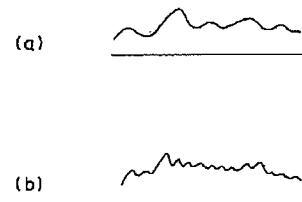
【符号の説明】

1…情報記録装置、2…課金対象情報入力部、3…ライセンス情報生成部、4…利用条件入力部、5…復号鍵入力部、6…鍵保持部、7…暗号化部、8…記録部、9…情報蓄積部、100…情報再生装置、101…情報蓄積部、102…読み出し部、103…復号ユニット、104…再生部、1001…情報記録装置、1002…ライセンス情報再生部、1003…情報記録部、1004…情報蓄積部、1011…情報記録装置、1012…読み出し部、1013…復号ユニット、1014…再生部、1015…情報蓄積部、2001…ライセンス情報入力部、2002…復号部、2003…判定部、2004…更新情報生成部、2005…鍵保持部、2006…鍵生成部、2007…時計参照部、2008…ライセンス情報更新装置、2009…利用条件入力部、2010…時計、2020…情報利用装置、3001…復号判定カード、3002…リムーバブルメディア読取装置、3003…リムーバブル情報蓄積メディア、3004…情報再生部、3005…時計、5001…ライセンス作成装置、5002…コンテンツデータベース(DB)、5003…ライセンス注入装置、5004…カードアダプタ、5005…プレーヤ、P…カード、D…レンタル用ディスク、7000…情報再生装置、7001…情報メディアドライバ、7002…情報利用装置、7008、8009…ライセンス判定ユニット、7101…再生装置、7102…会員カード、7103…情報記録メディア(ディスク)、7111…ライセンス／ポイント注入装置、7121…センター装置、8101…メディア、8102…メディア読取部、8103…復号ユニット、8110…カード、8112…表示装置、8121…放送波受信部(チューナ)。

【図5】



【図6】



```

graph TD
    ke1[課金対象情報 ke(1)] -- 2 --> Input1[課金対象情報 入力部]
    Input1 --> Recorder[記録部]
    Usage[使用条件] -- 4 --> Input2[使用条件 入力部]
    Key[復号鍵 kd(1)] --> Input3[復号鍵入力部]
    subgraph AdditionalInfoGen [付加情報生成部]
        Input2 --> Encrypt[暗号化部]
        Input3 --> Encrypt
    end
    KeyHolding[鍵保持部 ke] -- 6 --> Encrypt
    Encrypt -- 7 --> Recorder
    Recorder --> Storage[(情報蓄積部)]
    style AdditionalInfoGen fill:none,stroke-dasharray: 5 5
    style Storage fill:none,stroke-dasharray: 5 5
    subgraph Device [情報記録装置]
        Input1
        Recorder
    end

```

```

graph TD
    A[課金対象情報] -- 12 --> B[データ分離部]
    C[使用条件] -- 14 --> D[使用条件入力部]
    D -- 17 --> E[暗号化部]
    F[鍵保持部 k, e] -- 16 --> E
    B -- 18 --> G[記録部]
    E -- 18 --> G
    G -- 19 --> H[(情報蓄積部)]
    subgraph I [付加情報生成部]
        D
    end
    style I fill:none,stroke:#000
    style I stroke-width:2px
    
```

Figure 1 is a block diagram of the information recording device. The diagram shows the flow of data from input to storage. '課金対象情報' (Billing Target Information) is input to the 'データ分離部' (Data Separation Unit) via line 12. '使用条件' (Usage Conditions) is input to the '使用条件入力部' (Usage Condition Input Unit) via line 14. The '使用条件入力部' outputs to the '暗号化部' (Encryption Unit) via line 17. The '暗号化部' also receives input from the '鍵保持部 k, e' (Key Holding Unit k, e) via line 16. The 'データ分離部' outputs to the '記録部' (Recording Unit) via line 18. The '暗号化部' also outputs to the '記録部'. The '記録部' outputs to the '情報蓄積部' (Information Accumulation Unit) via line 19. The '付加情報生成部' (Additional Information Generation Unit) is shown as a sub-component that receives '使用条件' and outputs to the '暗号化部'. The entire system is labeled '情報記録装置' (Information Recording Device) at the bottom.

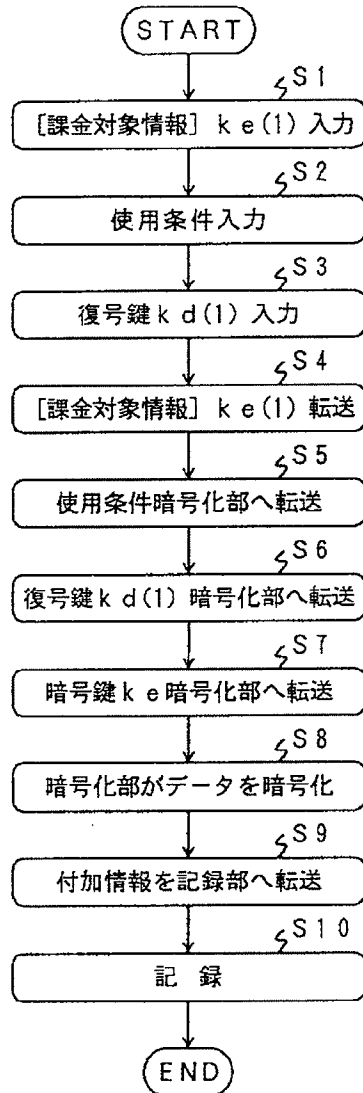
```

graph LR
    101[(情報記憶部)] --> 102[読み出し部]
    102 --> 103[復号ユニット]
    102 --> 105[復号部]
    103 --> 105
    105 --> 104[再生部]
    104 --> 表示[表示]
    subgraph 100 [情報再生装置]
        101
        102
        103
        104
        105
    end
  
```

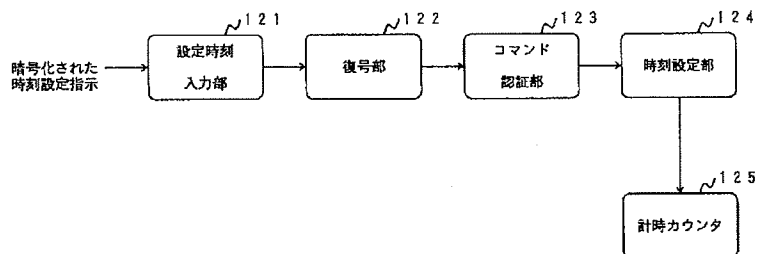
```

graph TD
    START([START]) --> ST1[時刻入力]
    ST1 --> ST2[時刻設定指示]
    ST2 --> ST3[時刻設定]
    ST3 --> ST4[時刻設定無効化指示]
    ST4 --> ST5[時刻設定無効化部が時刻設定を無効化]
    ST5 --> END([END])
  
```

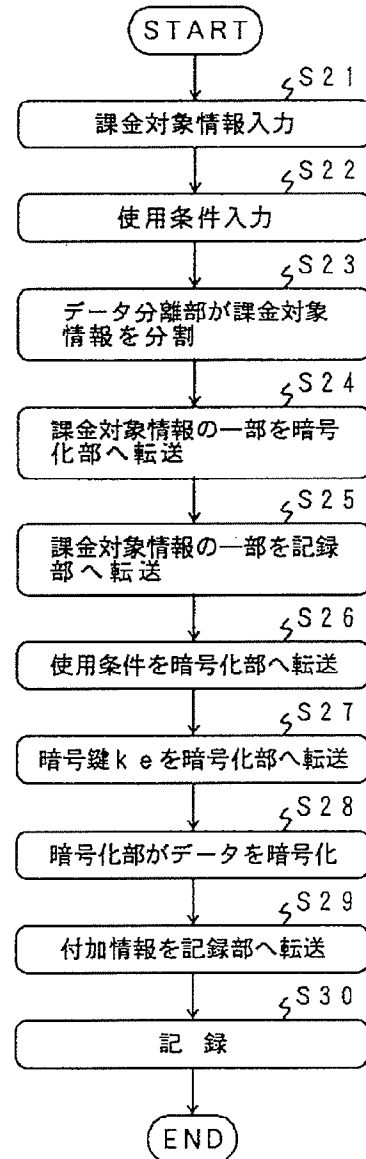
【図2】



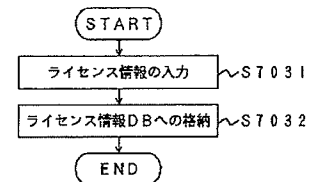
【図15】



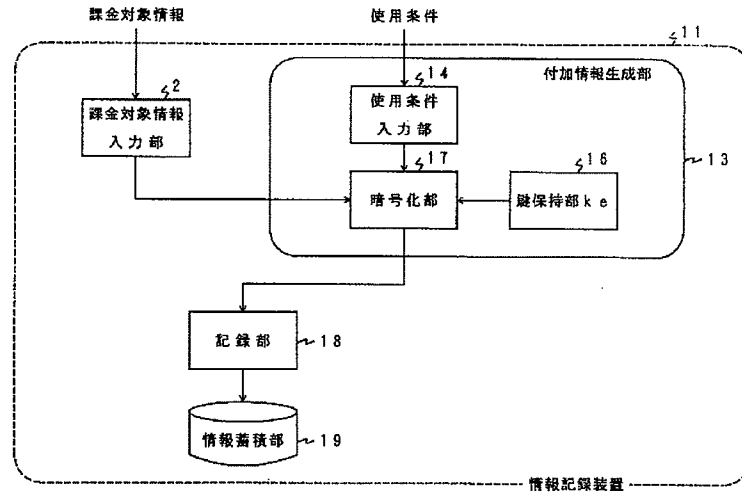
【図4】



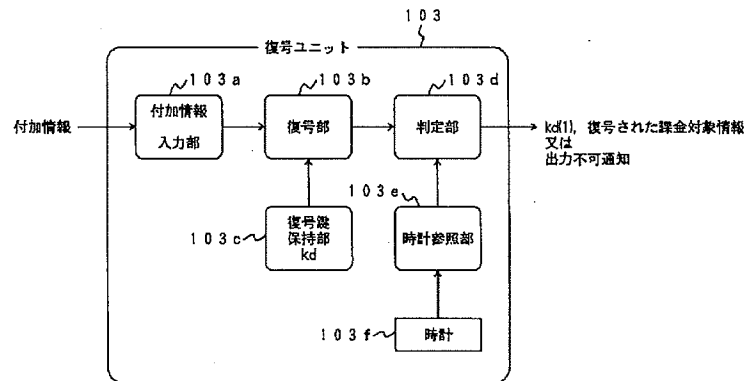
【図111】



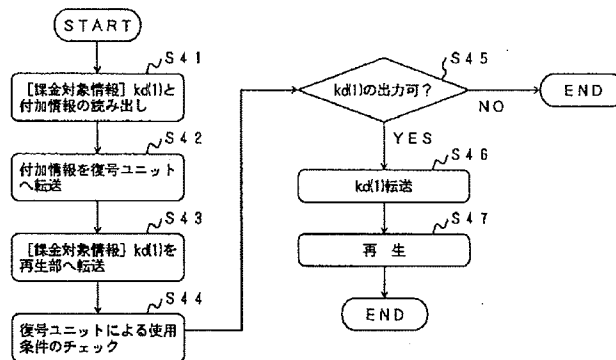
【図7】



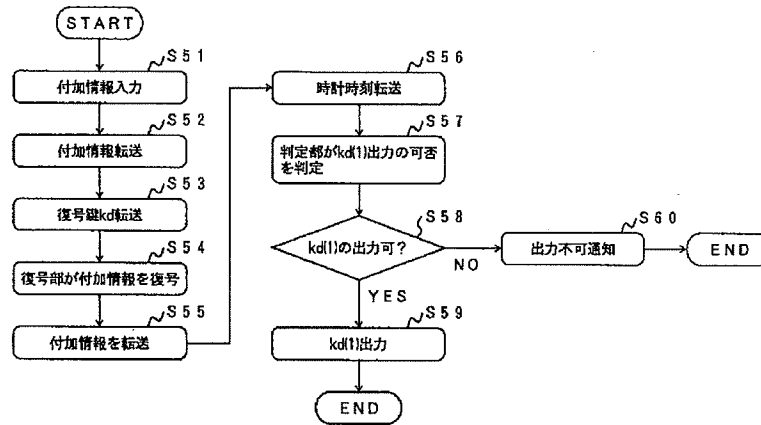
【図9】



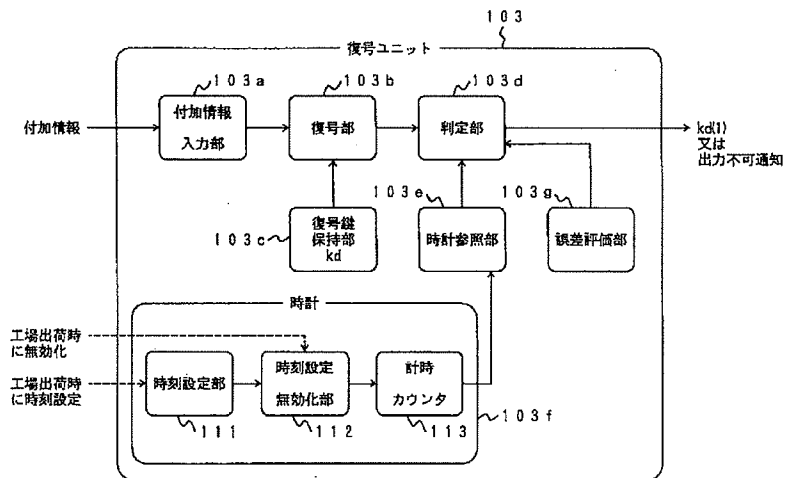
【図10】



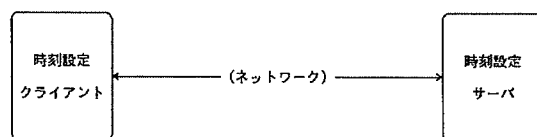
【図11】



【図12】

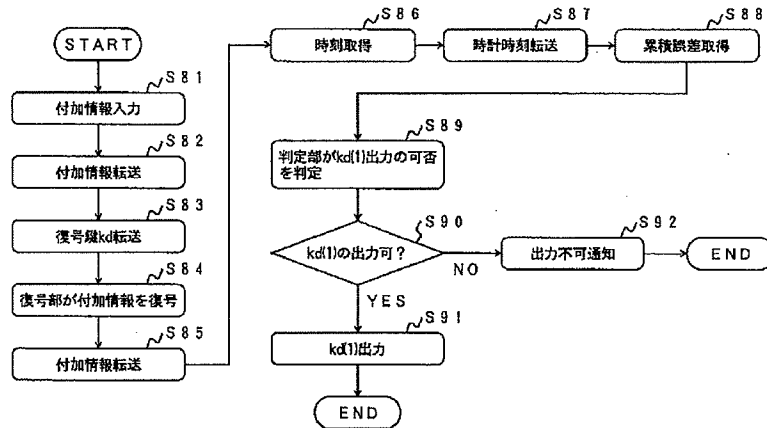


【図17】

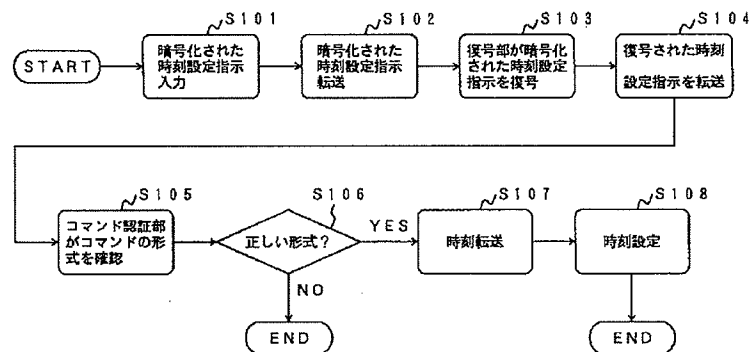




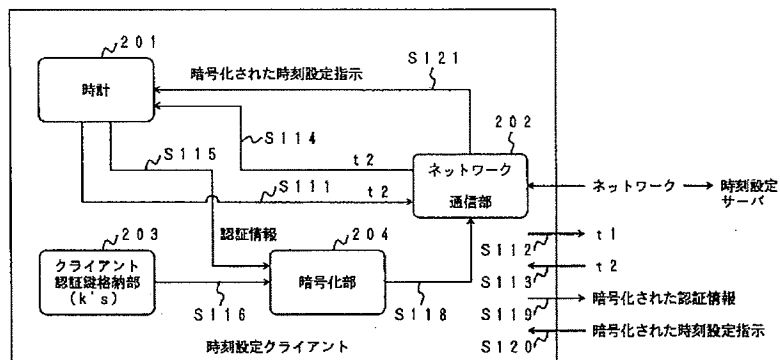
【図14】



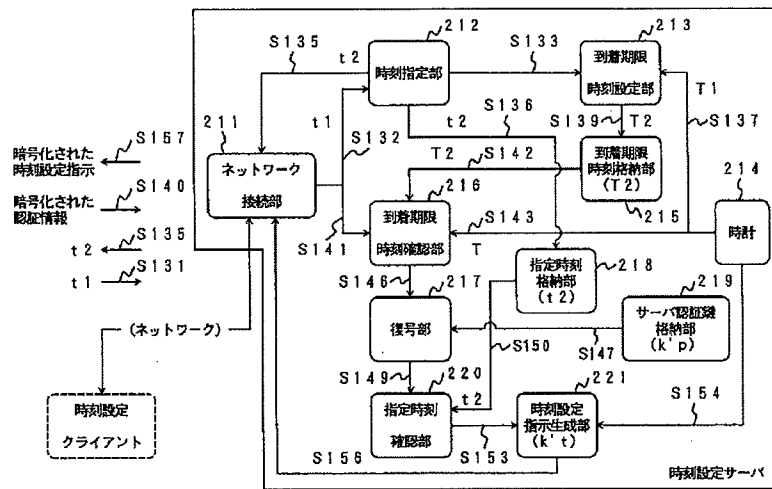
【図16】



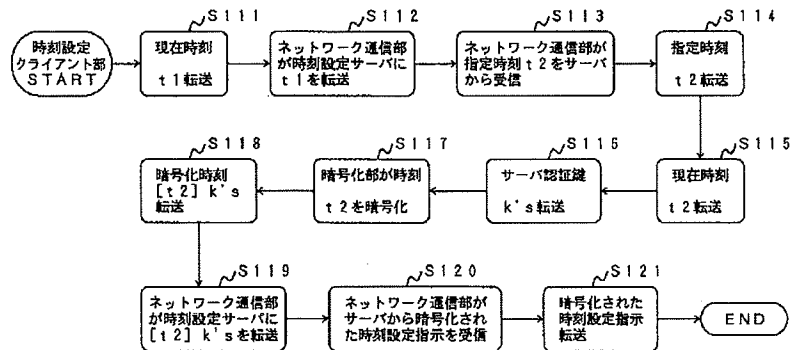
【図18】



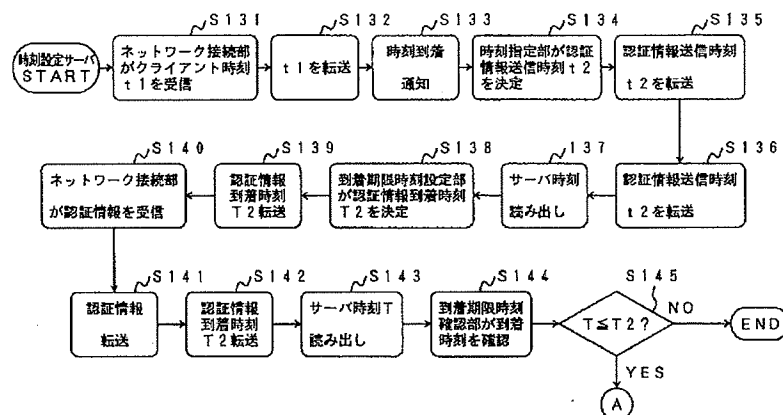
【図19】



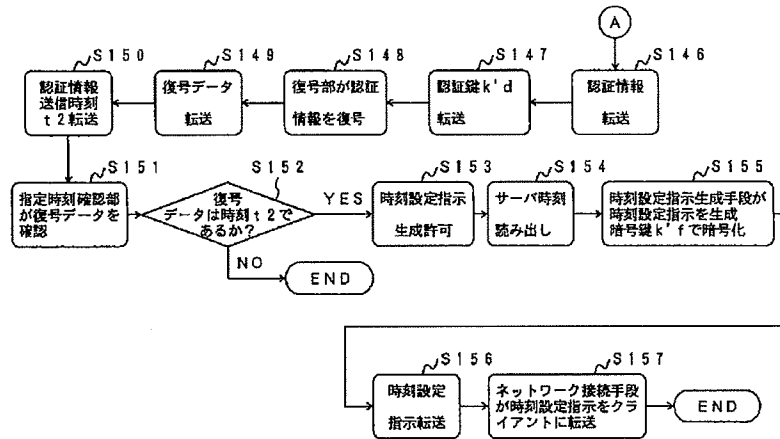
【図20】



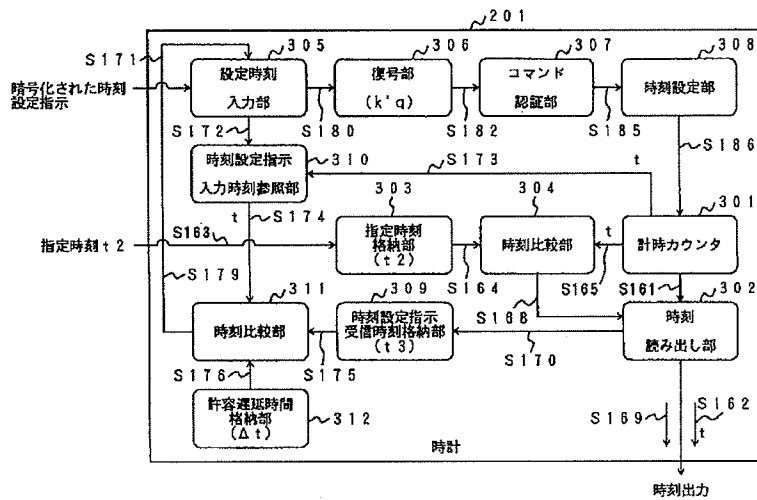
【図21】



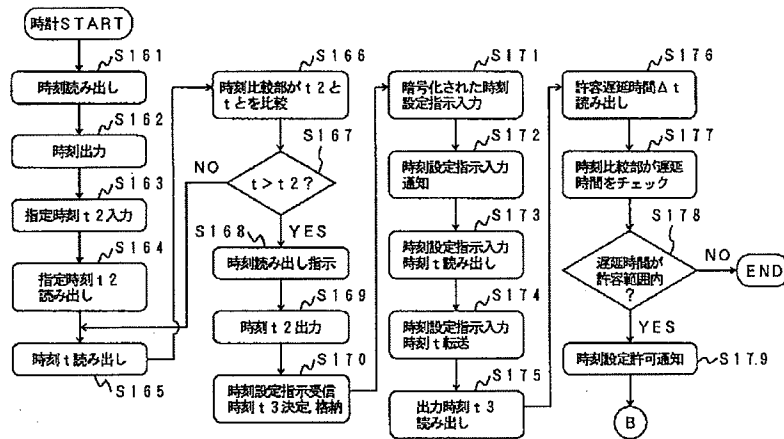
【図22】



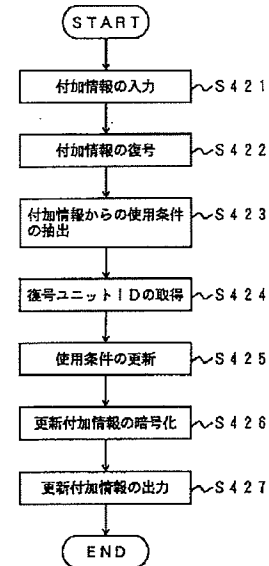
【図23】



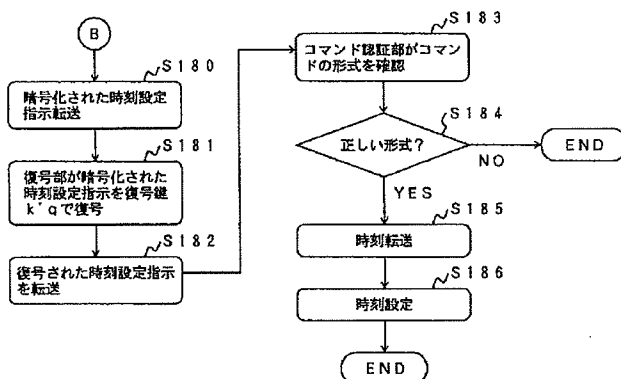
【図24】



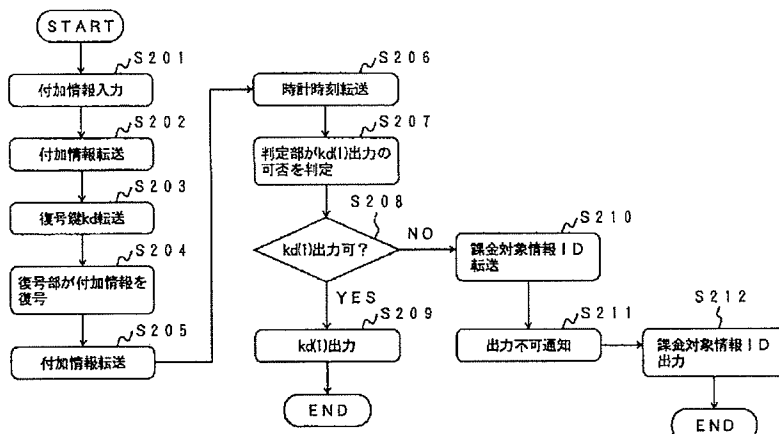
【図42】



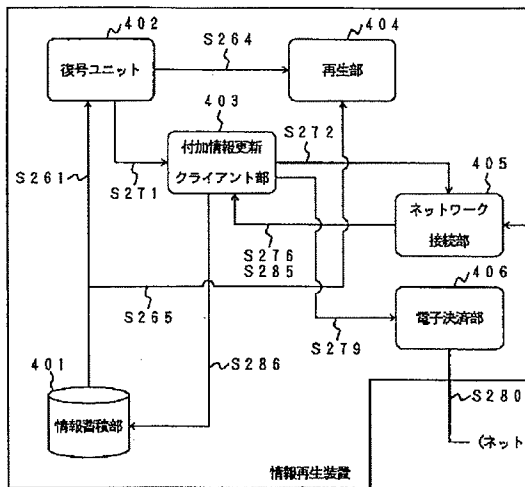
【図25】



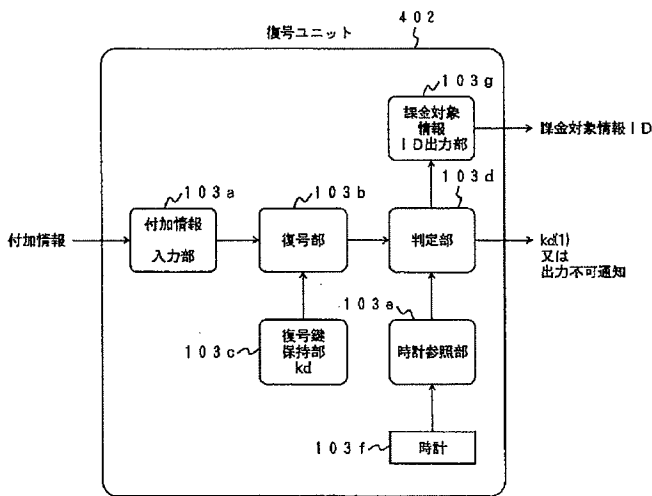
【図28】



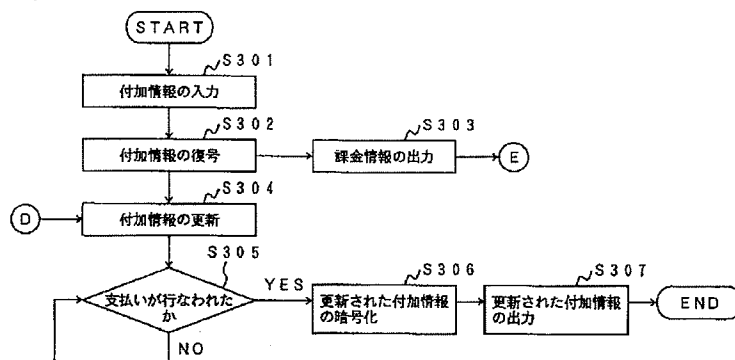
【図26】



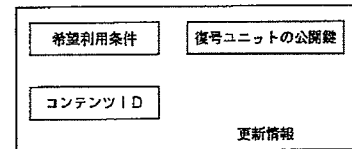
【図27】



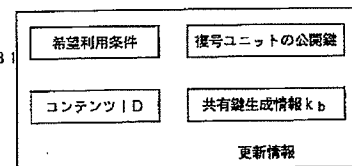
【図36】



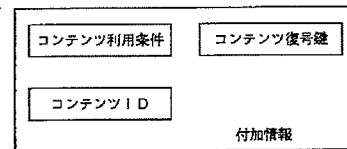
【図56】



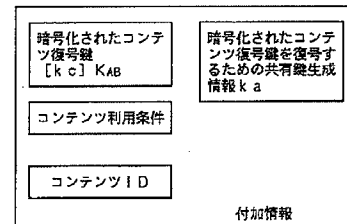
【図64】



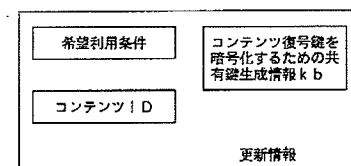
【図55】



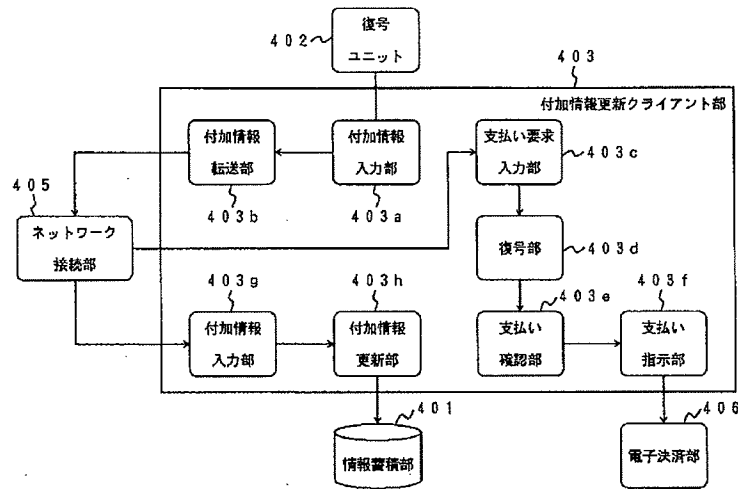
【図60】



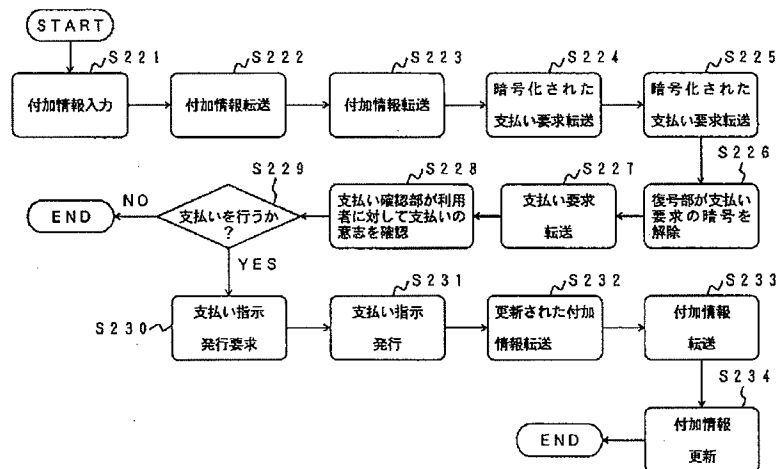
【図62】



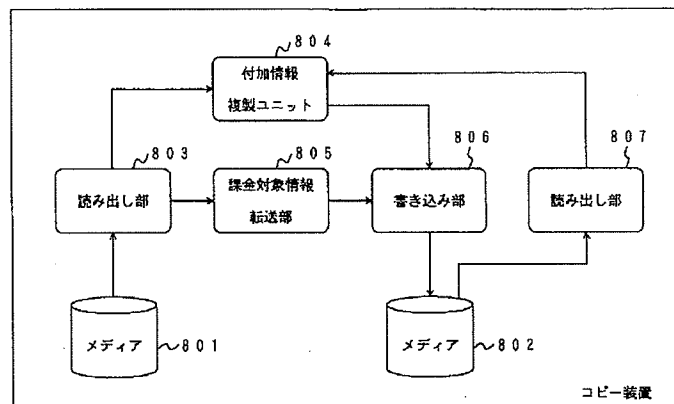
【図29】



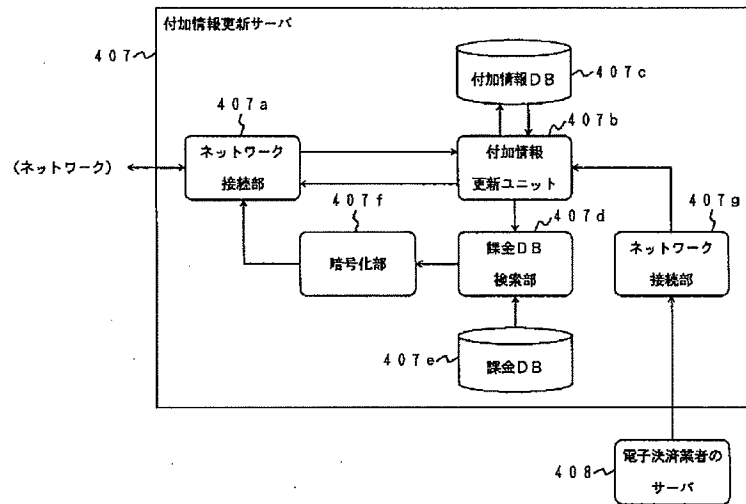
【図30】



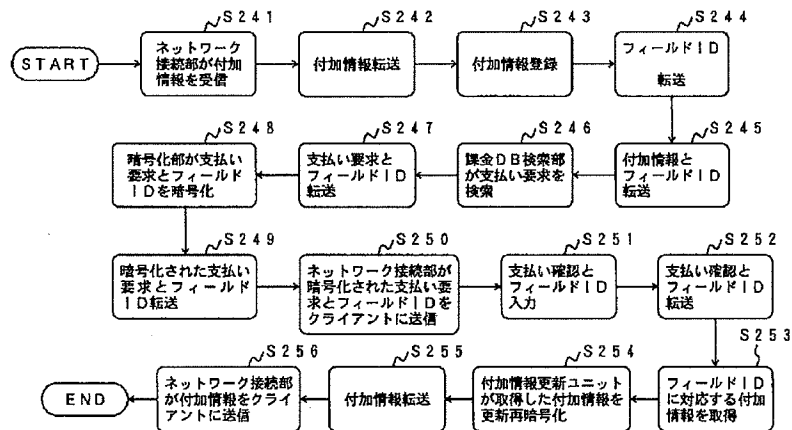
【図45】



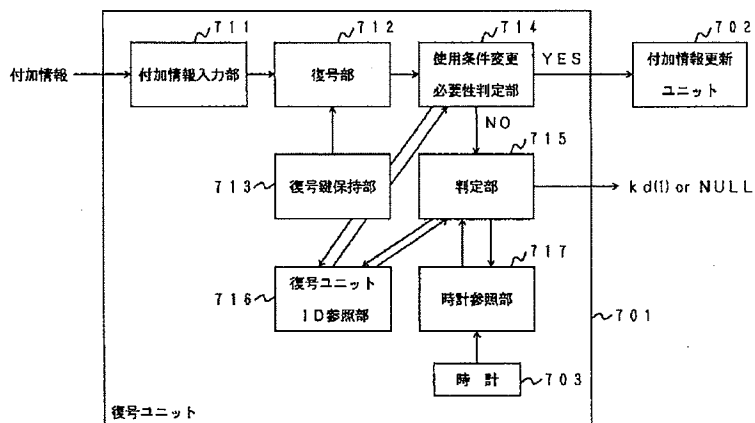
【図31】



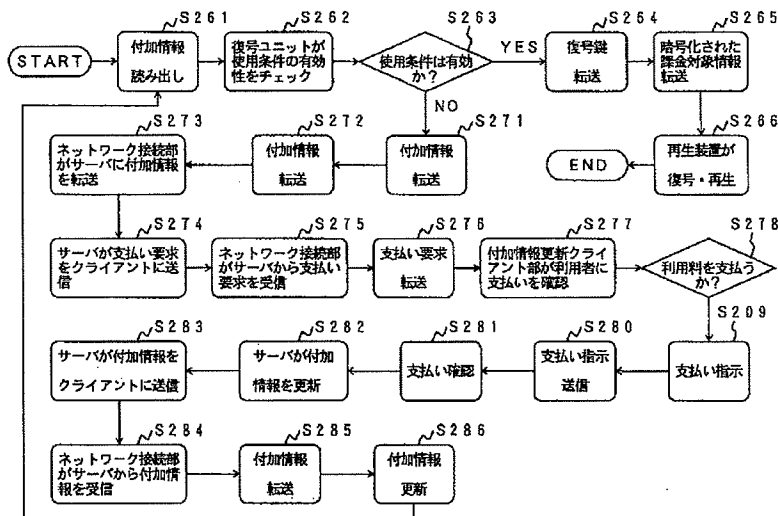
【図32】



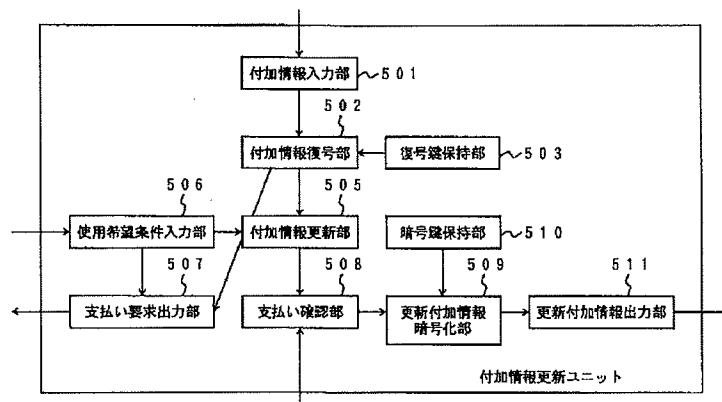
【図39】



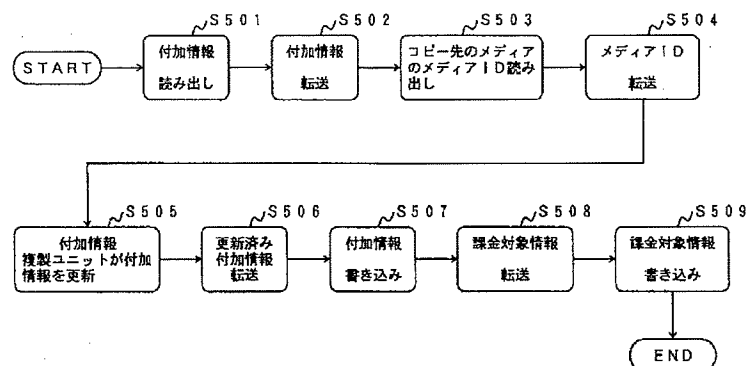
【図34】



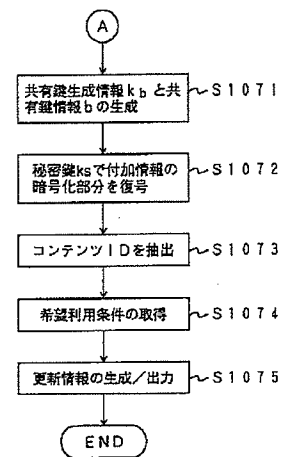
【図35】



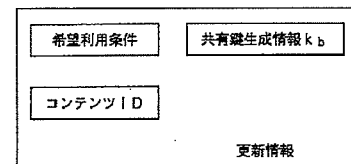
【図46】



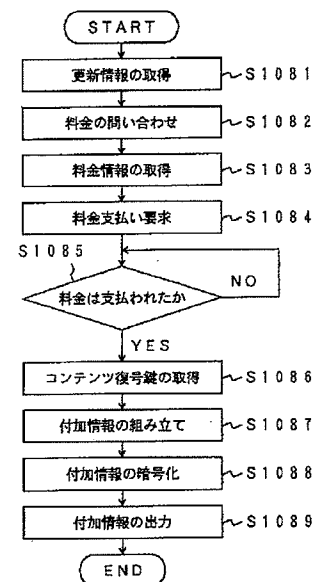
【図68】



【図69】

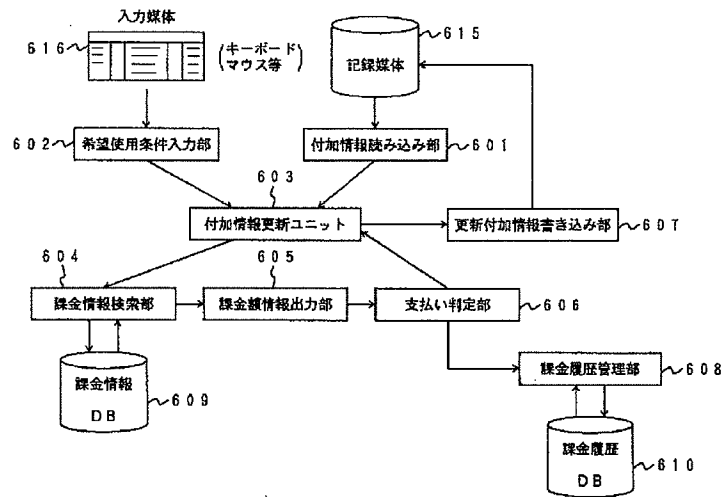


【図72】

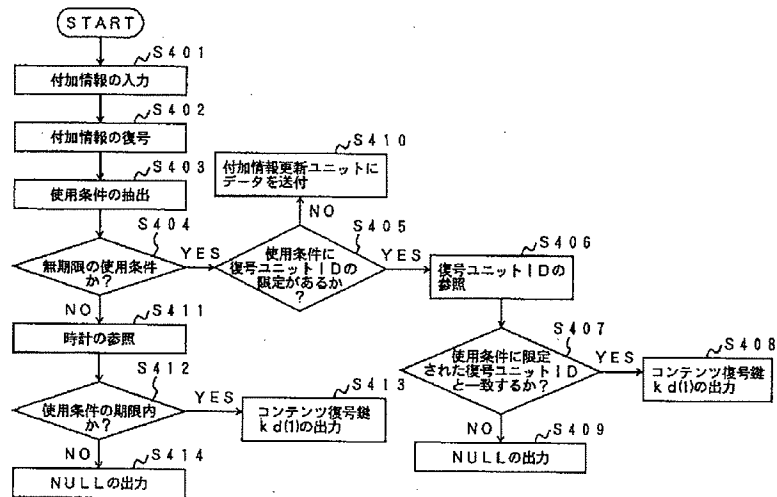




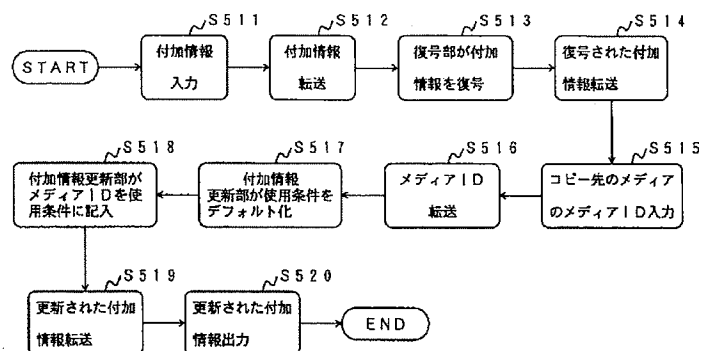
【図38】



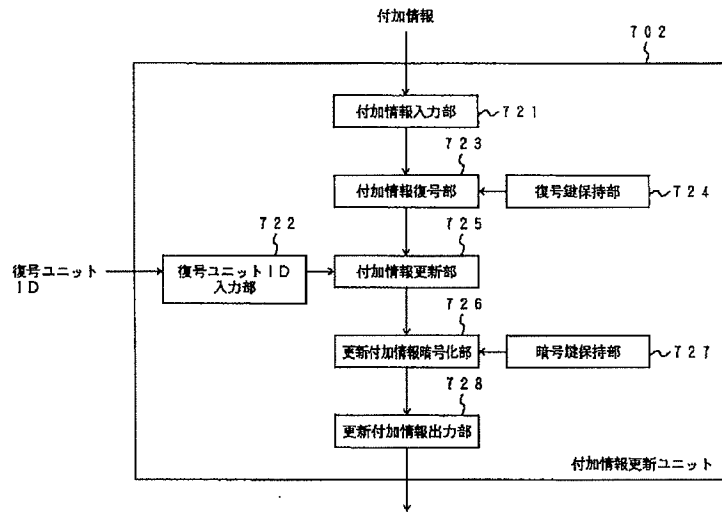
【図40】



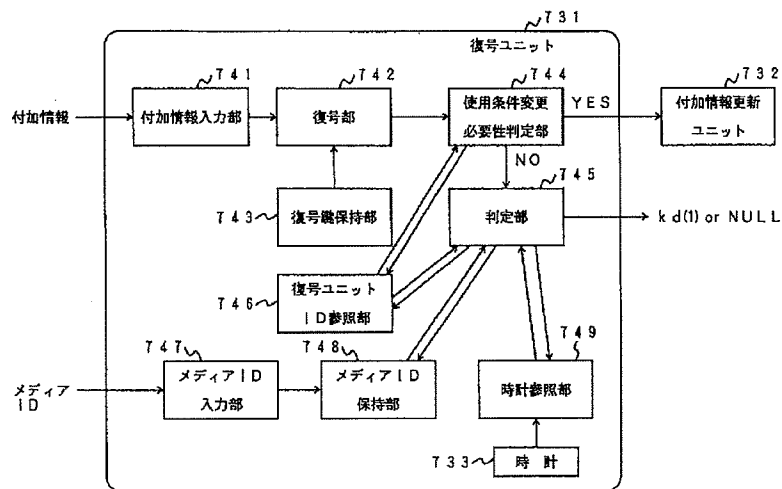
【図48】



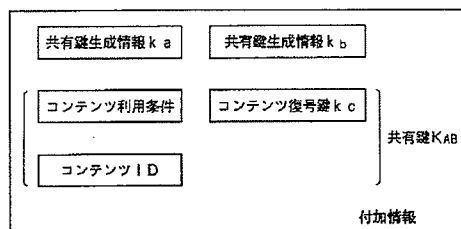
【図41】



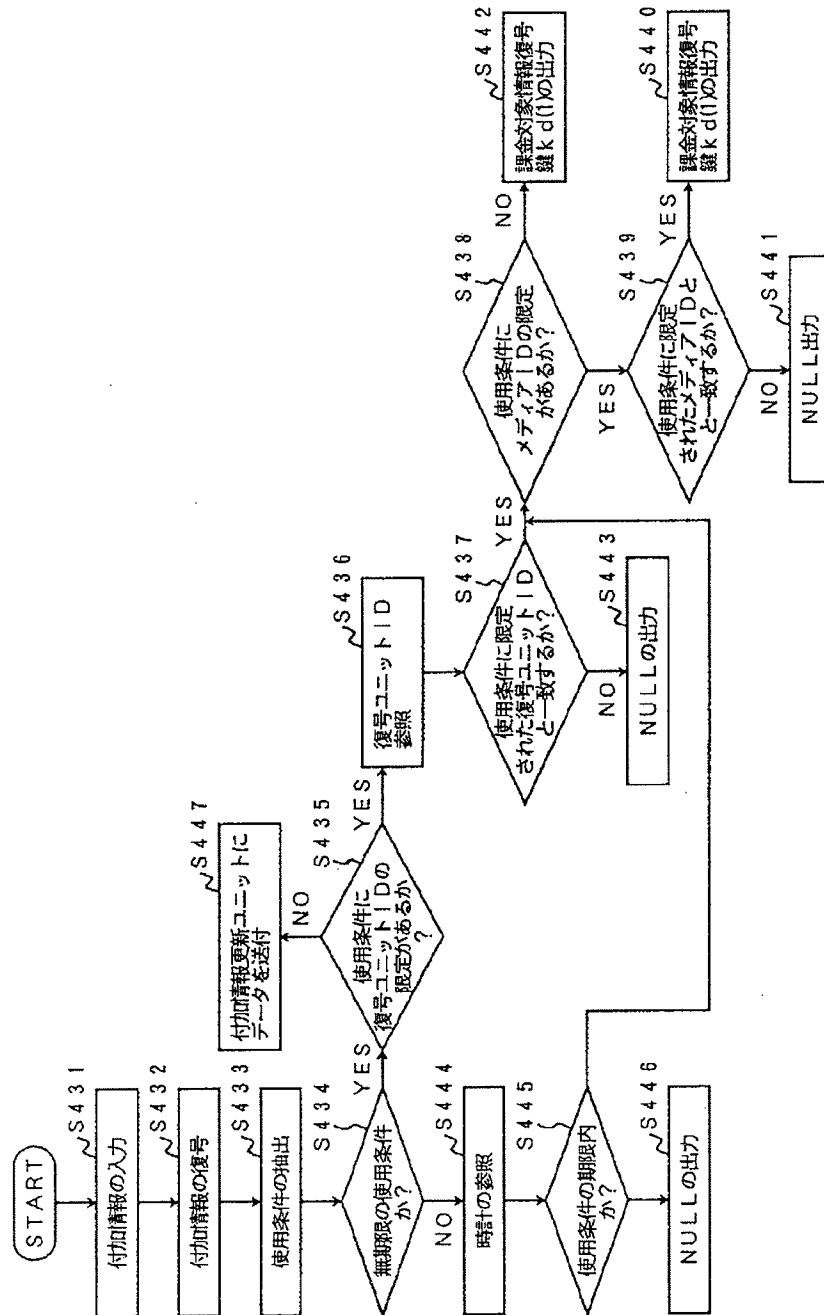
【図43】



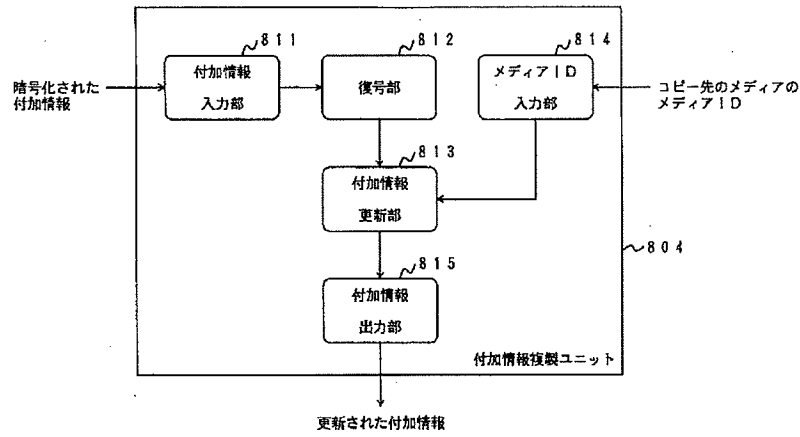
【図66】



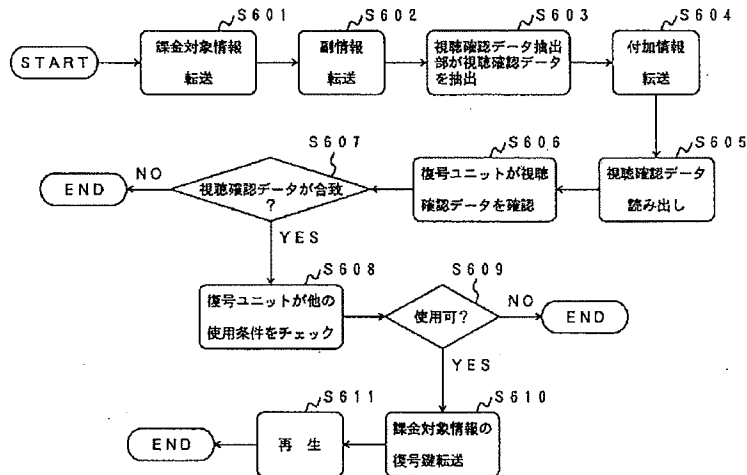
【図44】



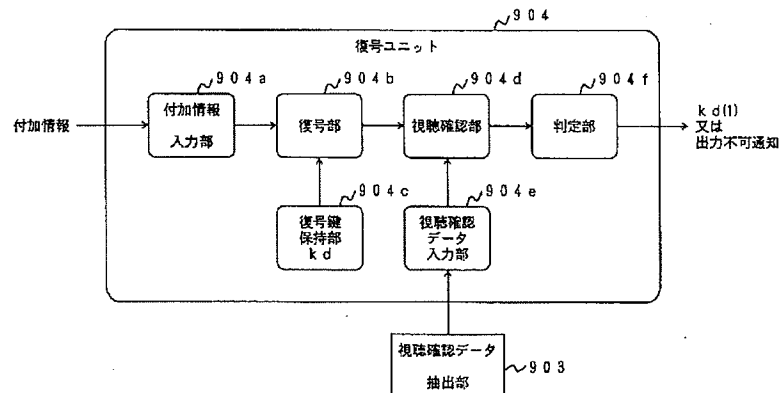
【図47】



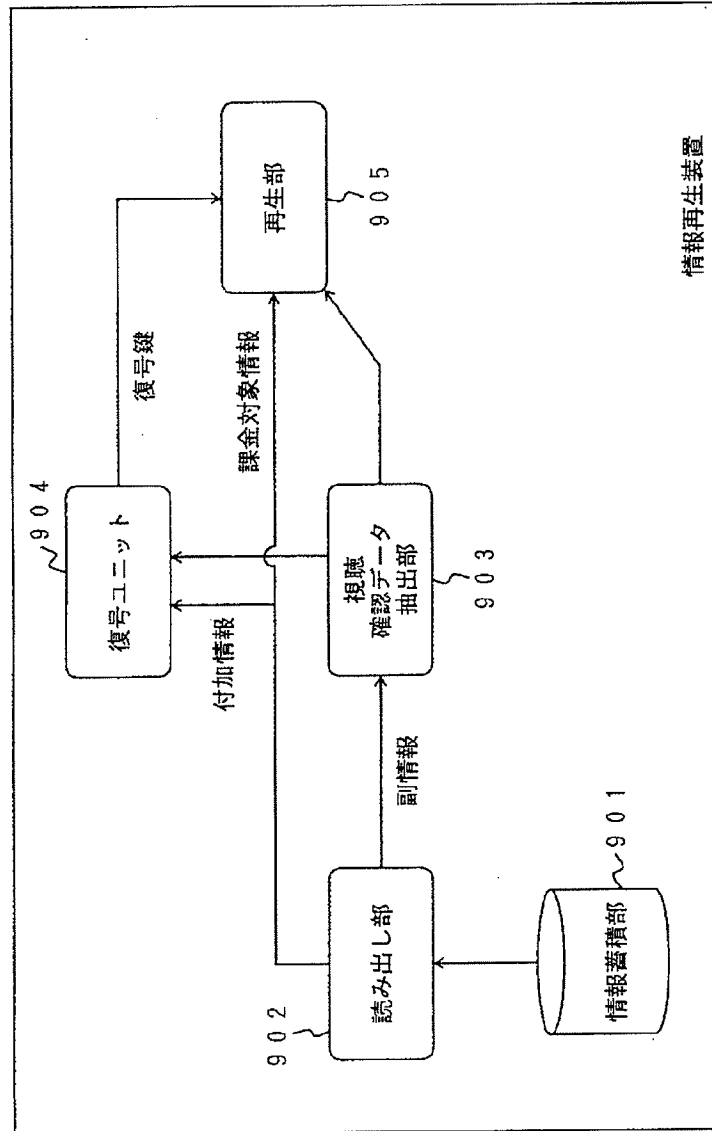
【図50】



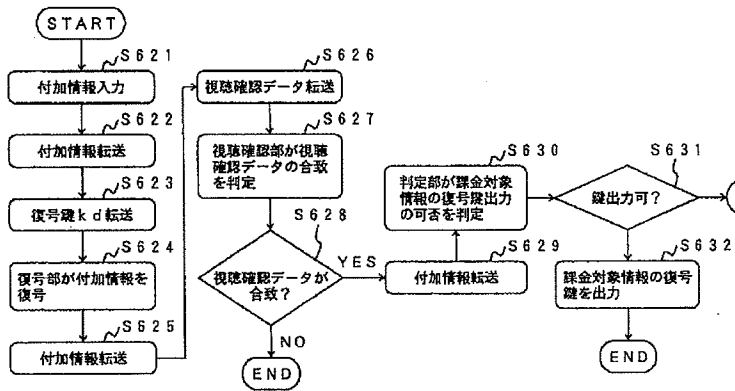
【図51】



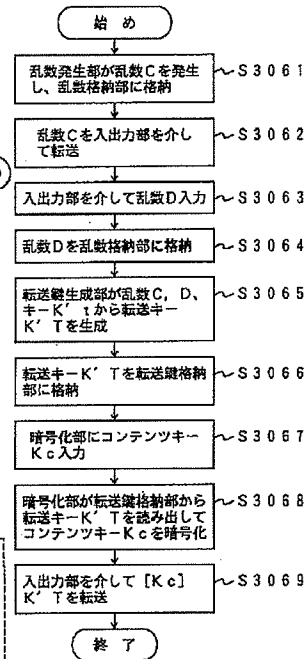
【図49】



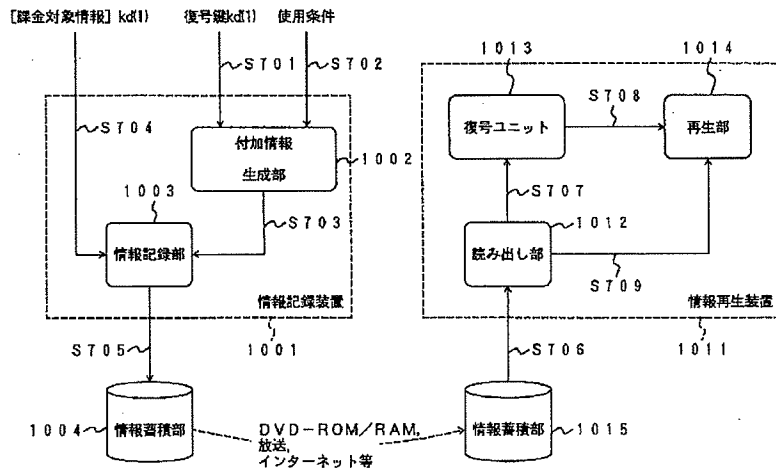
【図52】



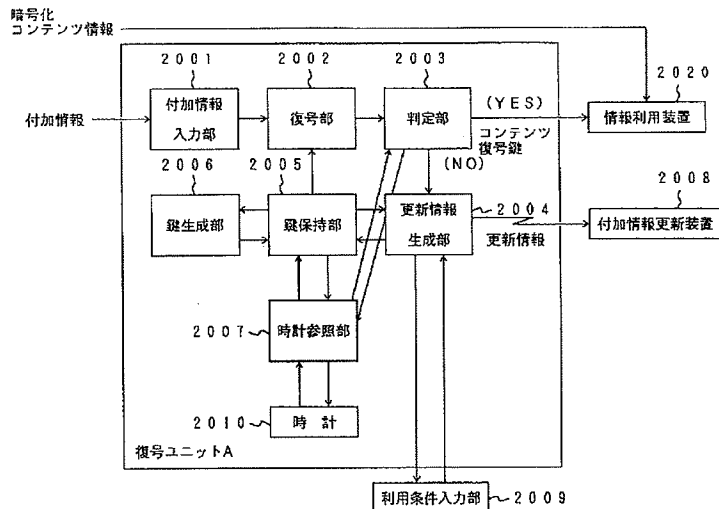
【図86】



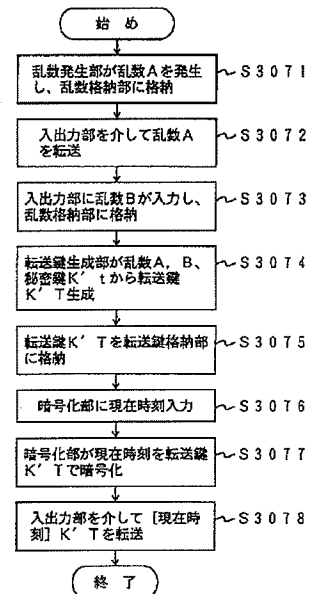
【図53】



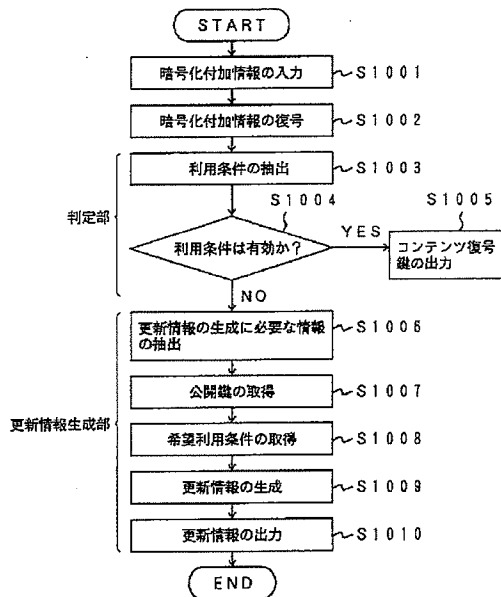
【図54】



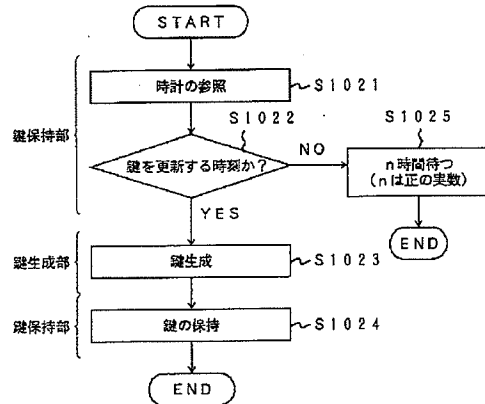
【図89】



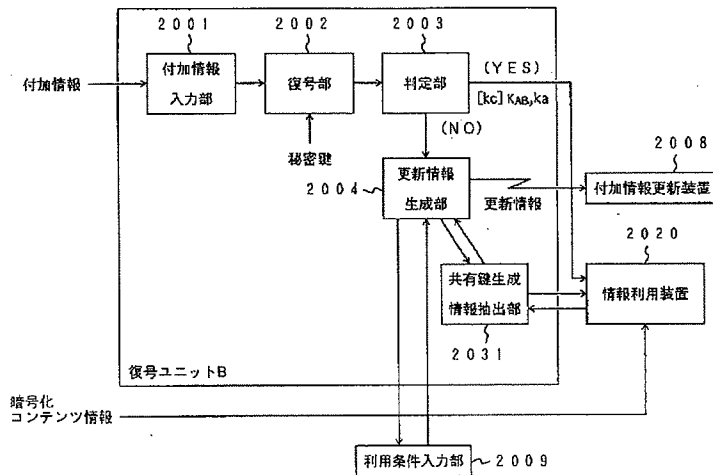
【図57】



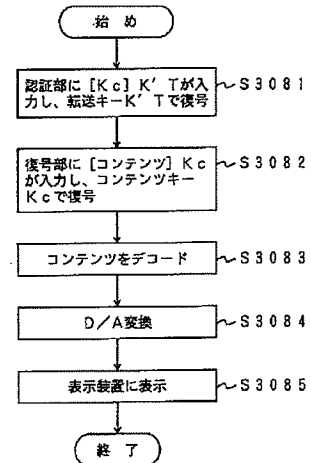
【図58】



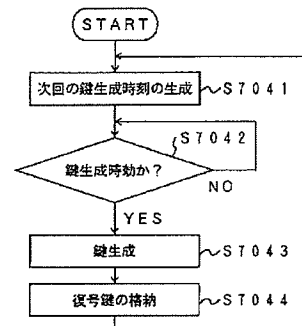
【図59】



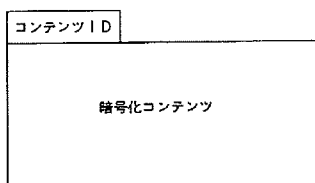
【図93】



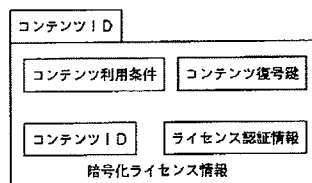
【図112】



【図113】



【図115】



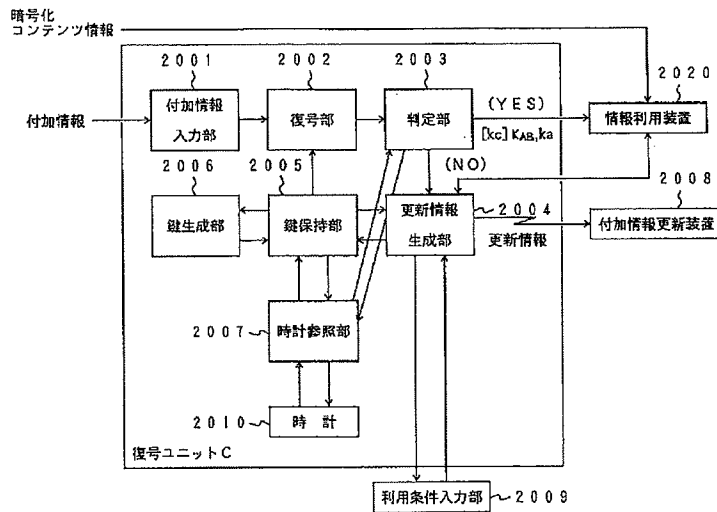
```

graph TD
    START([START]) --> S1031[暗号化付加情報の入力]
    S1031 --> S1032[暗号化付加情報の復号]
    S1032 --> S1033[利用条件の抽出]
    S1033 --> S1034{利用条件は有効か?}
    S1034 -- YES --> S1035[暗号化されたコンテンツ復号鍵 [k c] KAB及び共有鍵生成情報 ka の出力]
    S1034 -- NO --> S1036[更新情報の生成に必要な情報の抽出]
    S1036 --> S1037[共有鍵生成情報の抽出]
    S1037 --> S1038[希望利用条件の取得]
    S1038 --> S1039[更新情報の生成]
    S1039 --> S1040[更新情報の出力]
    S1040 --> END([END])

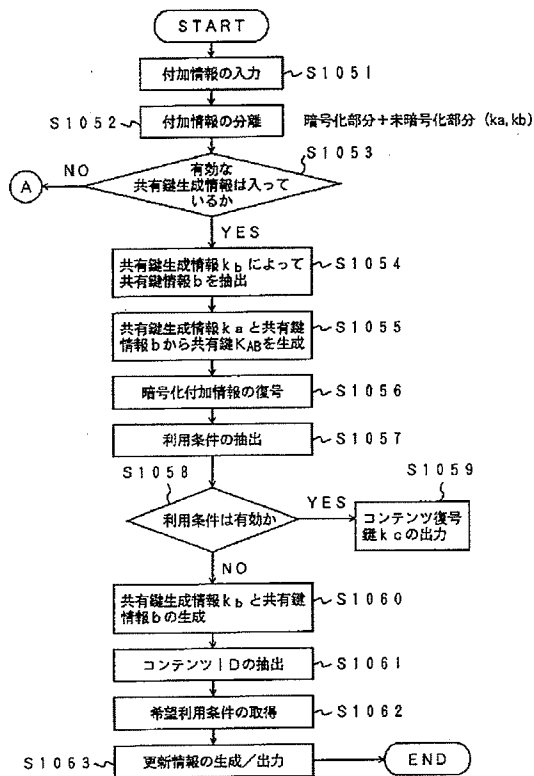
```



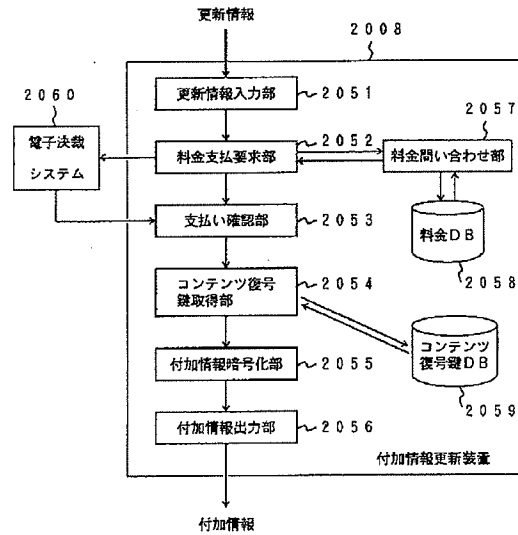
【図63】



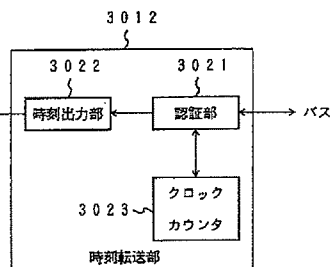
【図67】



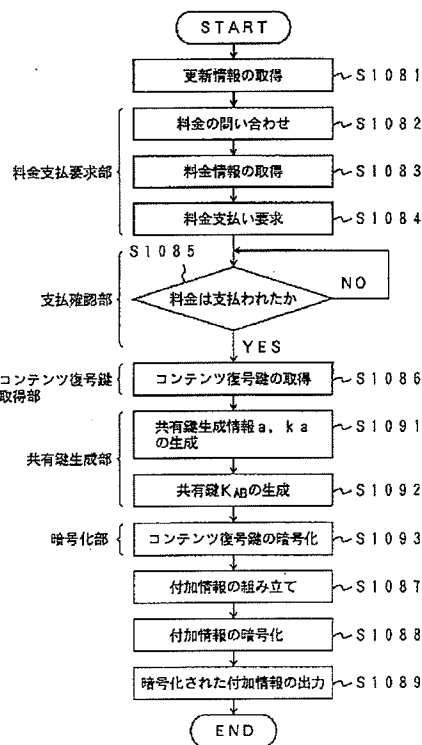
【図71】



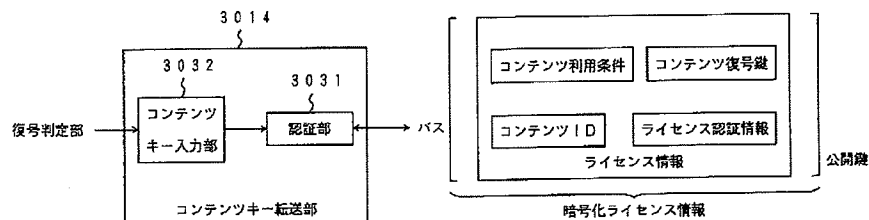
【图81】



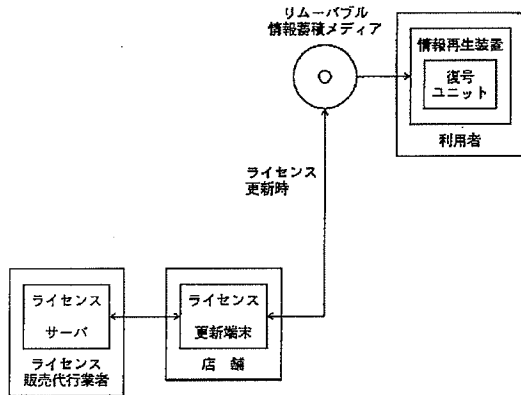
【图74】



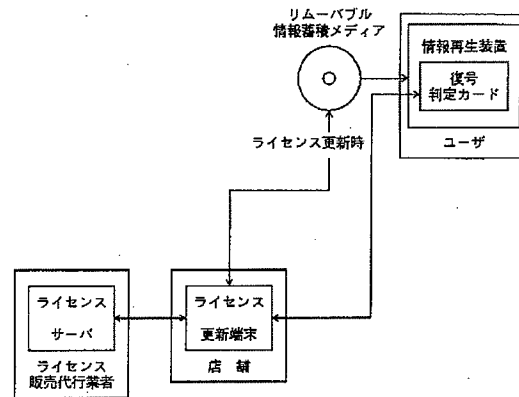
【图 1 1 4】



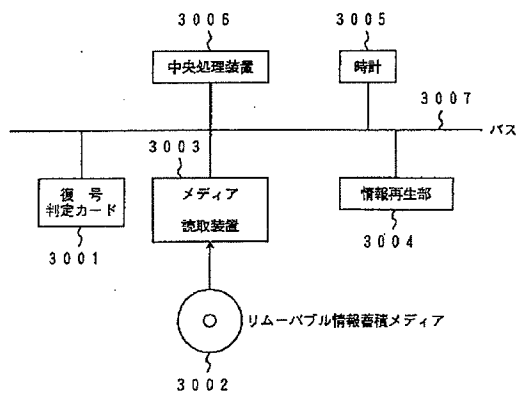
【図75】



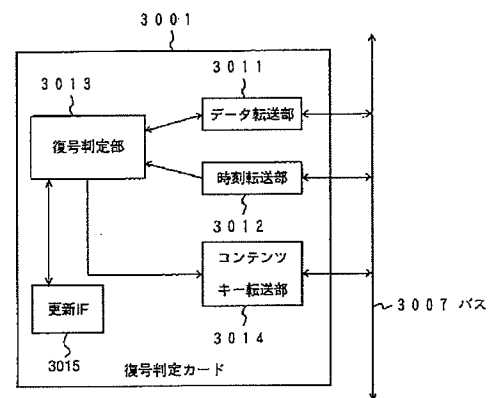
【図76】



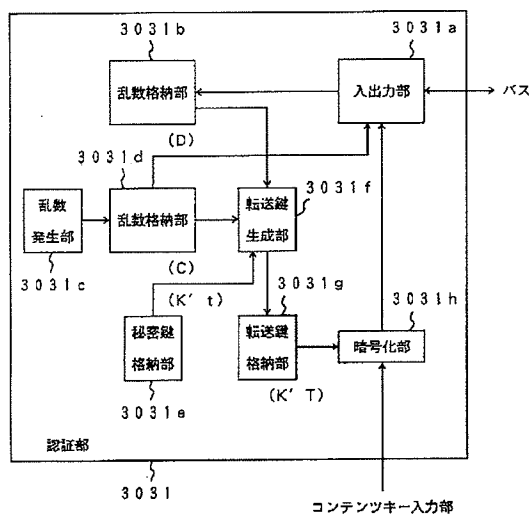
【図77】



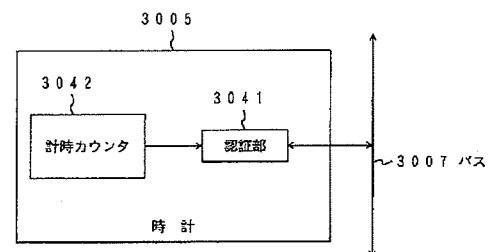
【図79】



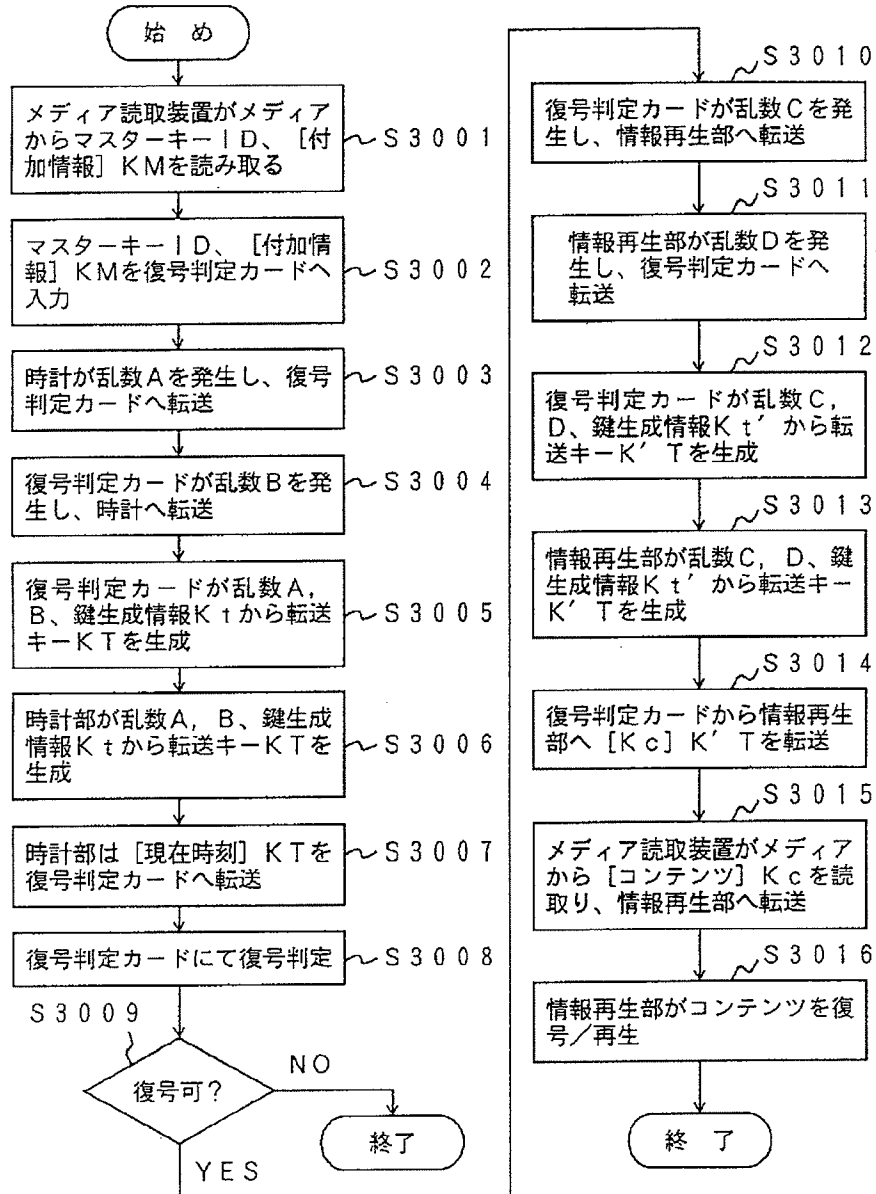
【図85】



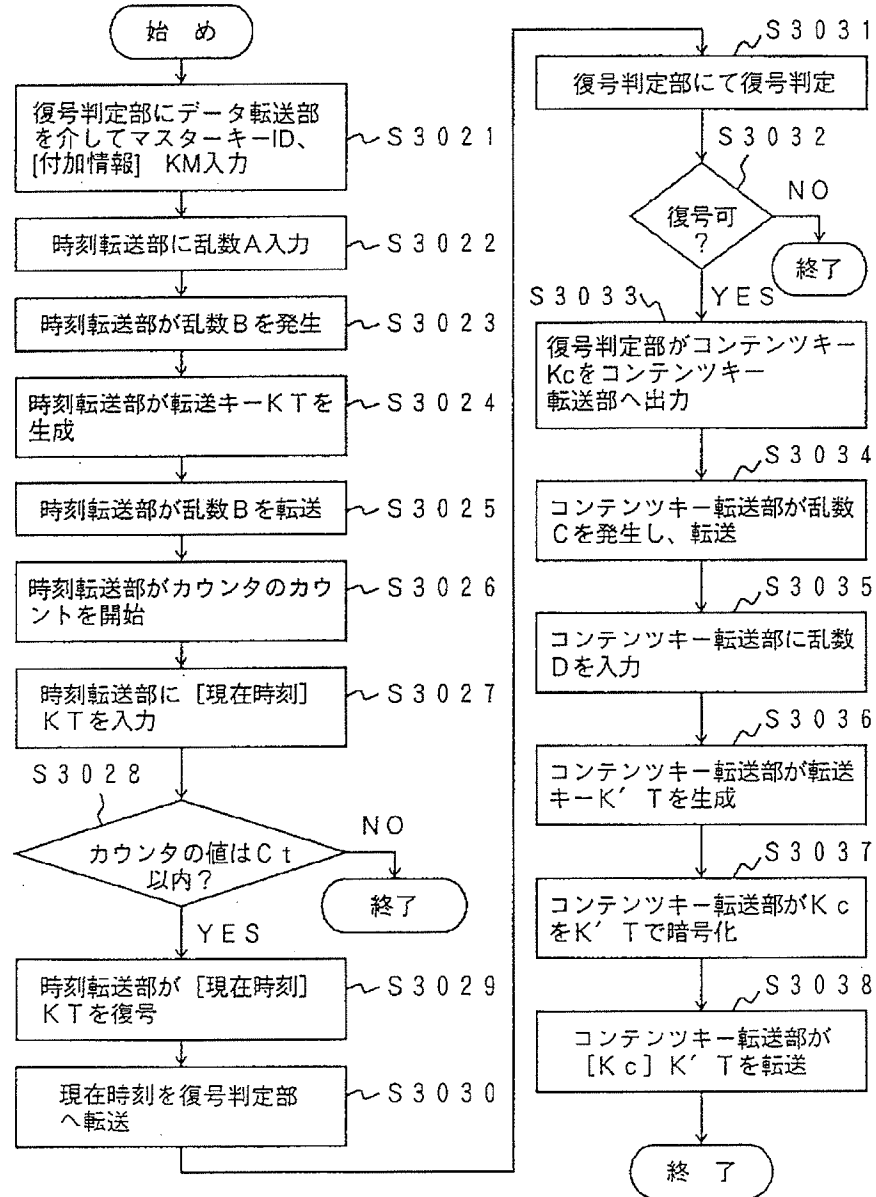
【図87】



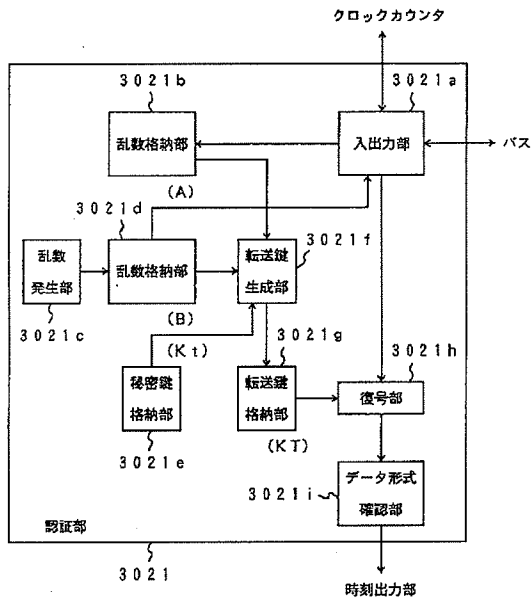
【図78】



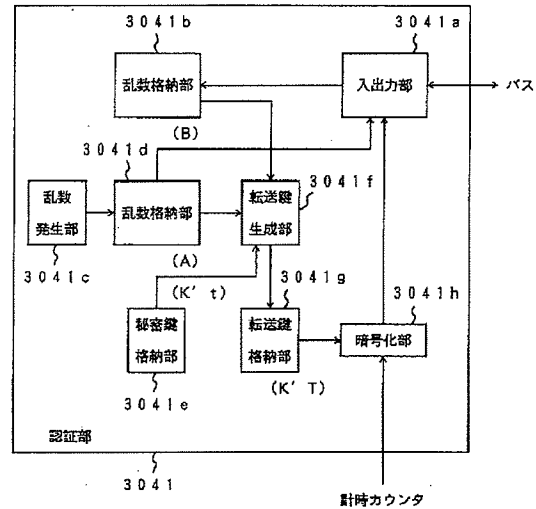
【図80】



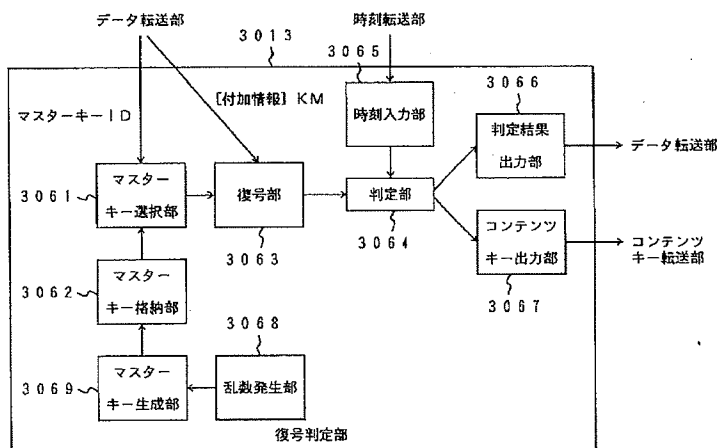
【図82】



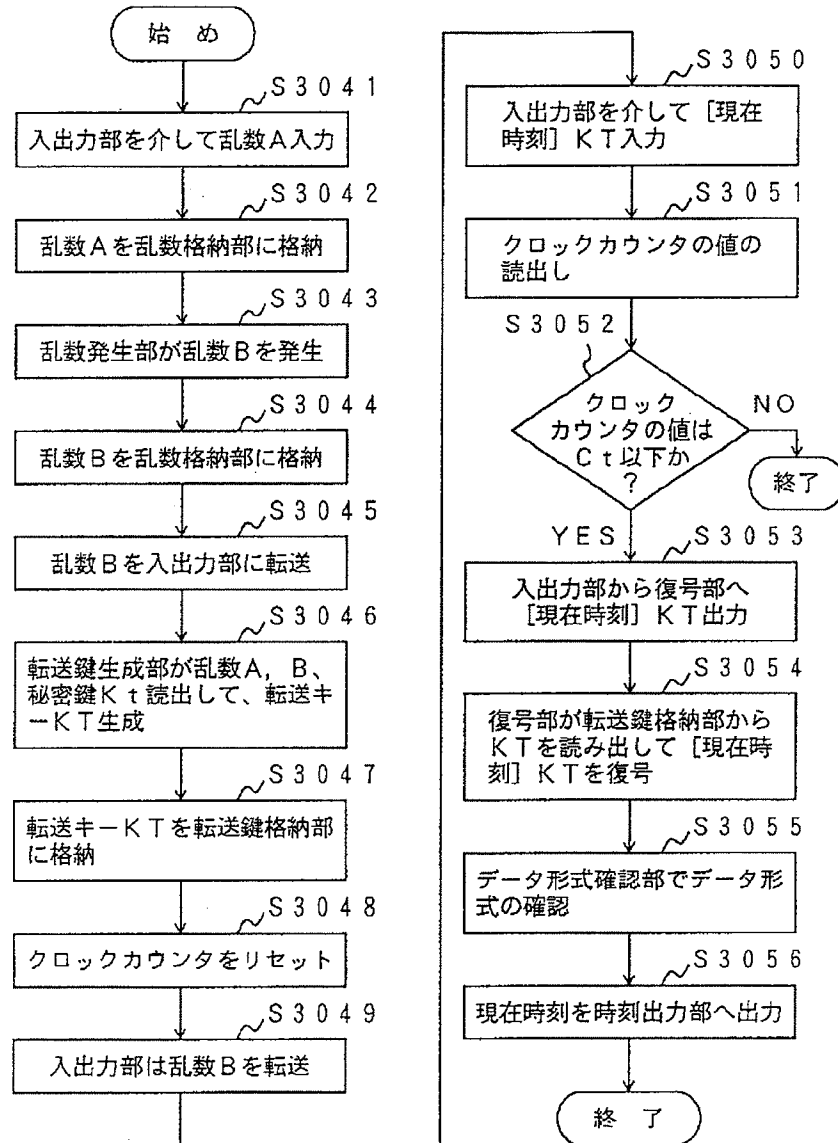
【図88】



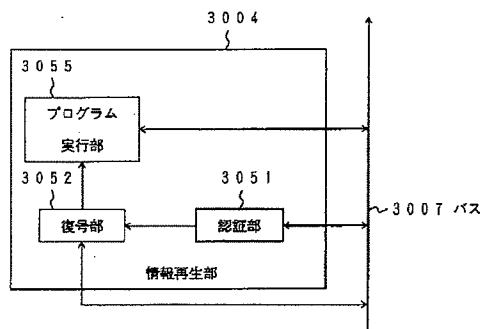
【図90】



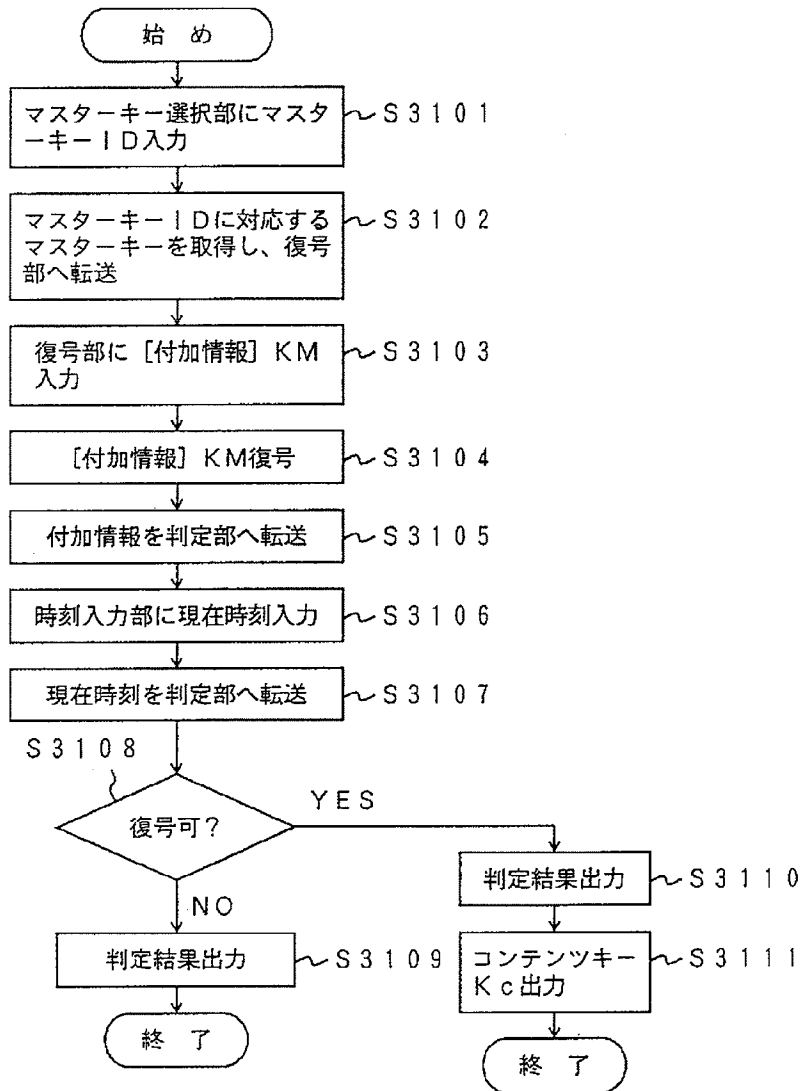
【図83】



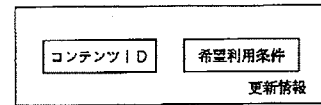
【図96】



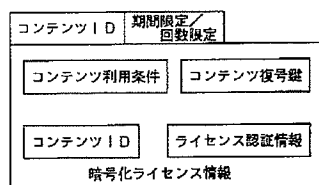
【図91】



【図116】

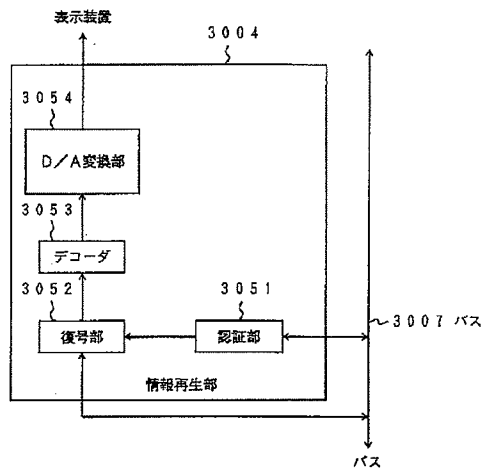


【図117】

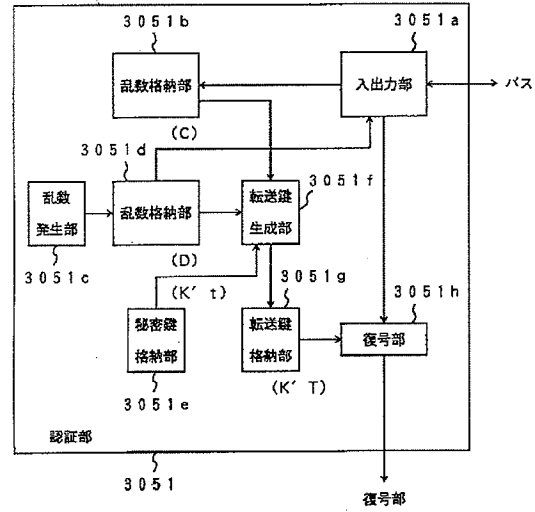




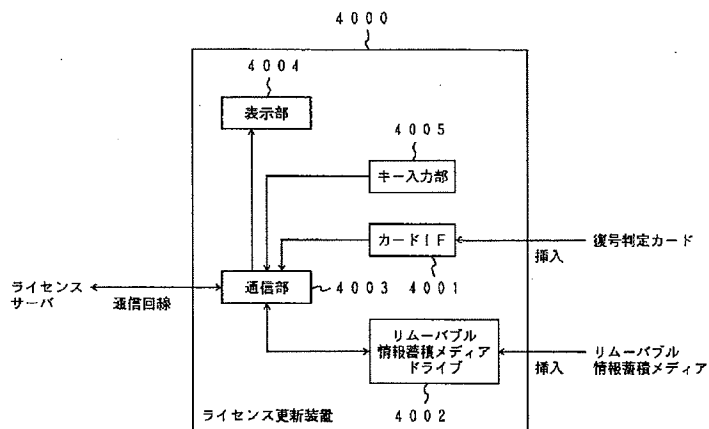
【図92】



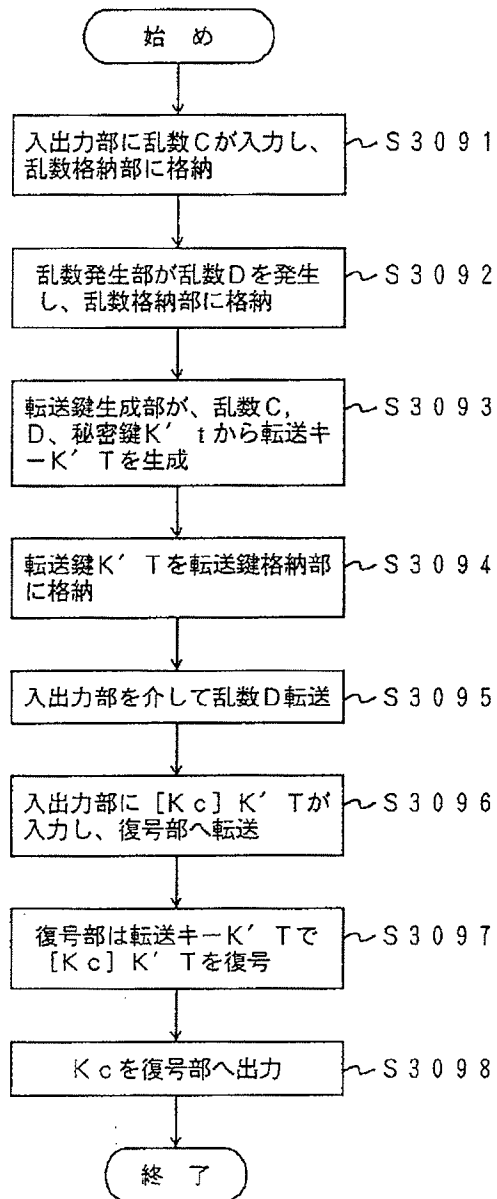
【図94】



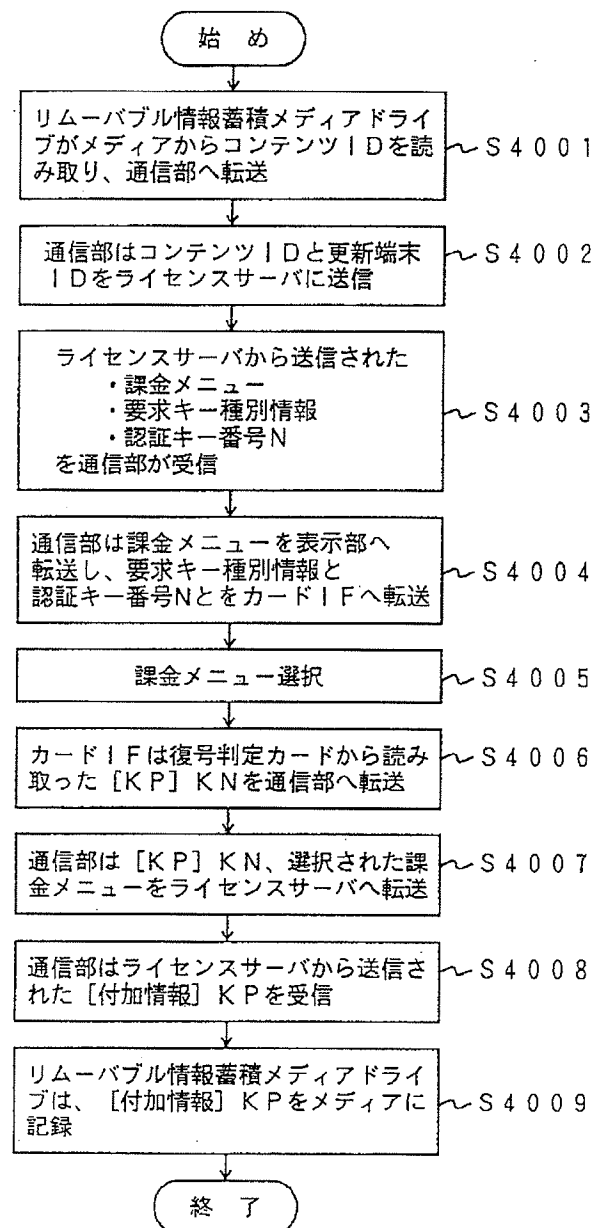
【図97】



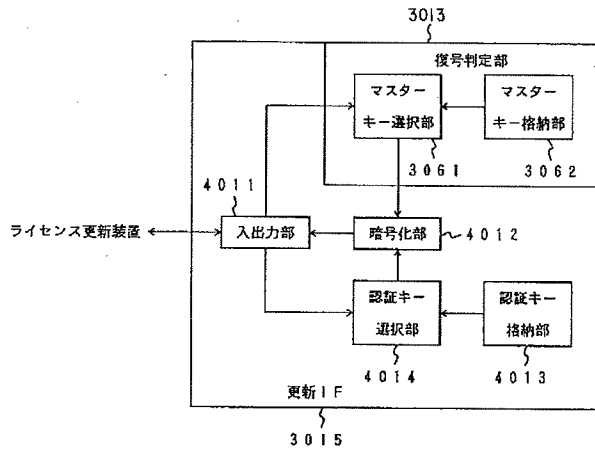
【図95】



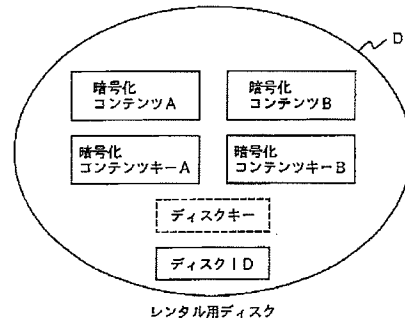
【図98】



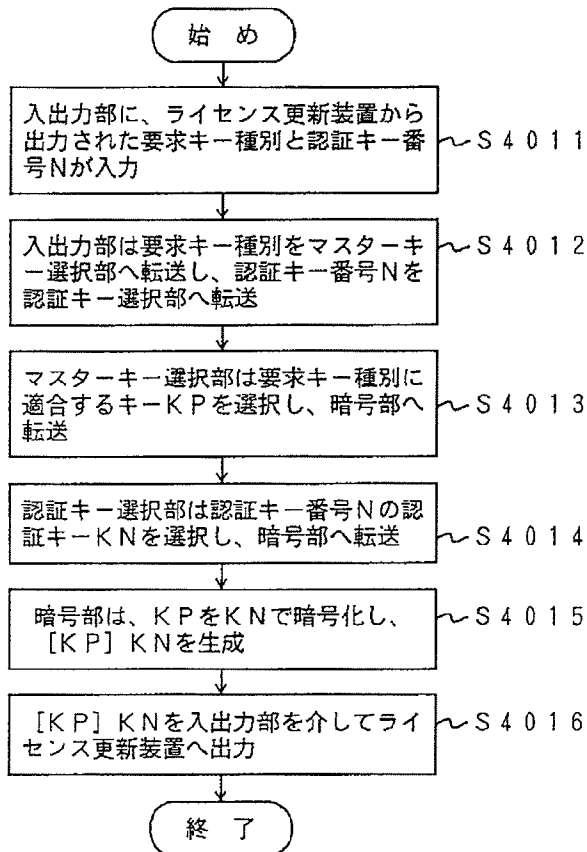
【図99】



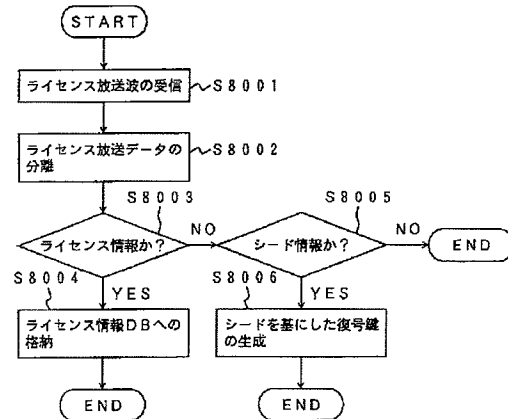
【図123】



【図100】



【図120】

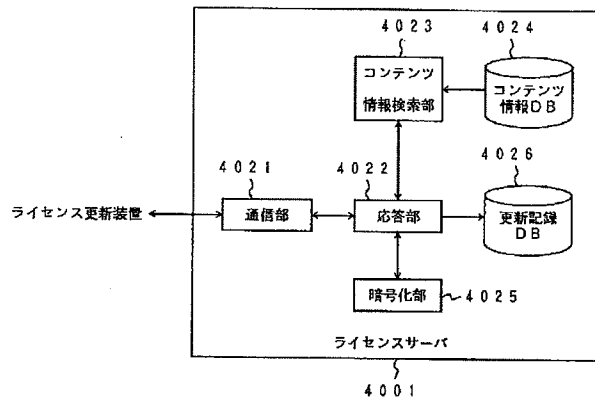


【図124】

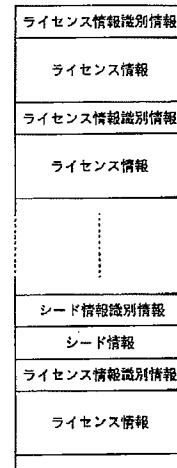
ディスクID	ディスクキー
000102	1768afdd5
000103	465effaab89
...	...

コンテンツDB

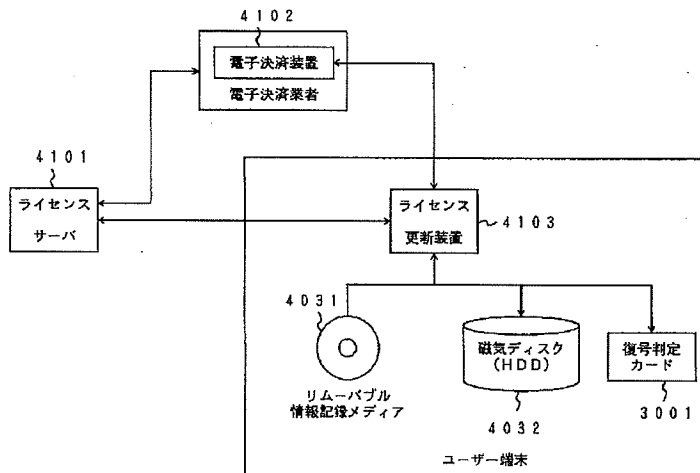
【図101】



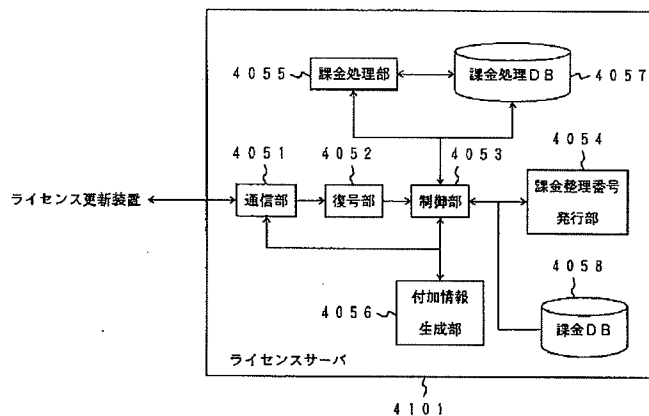
【図121】



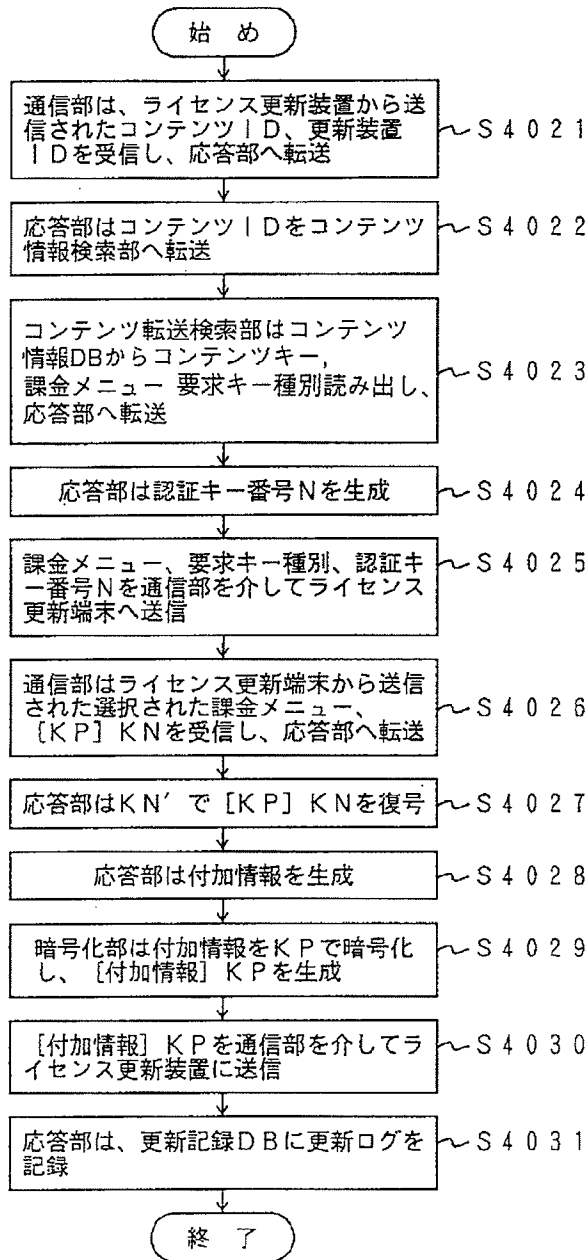
【図103】



【図105】



【図102】

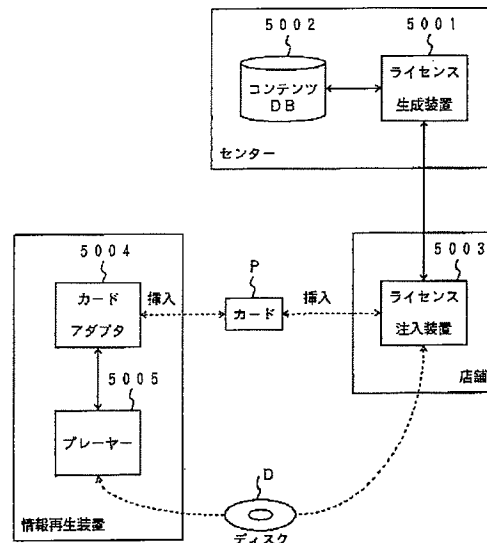


【図132】

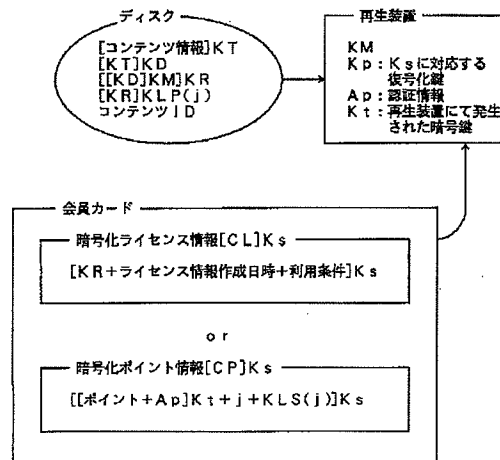
ディスクID	暗号化ディスク情報
0809eefd32	Fexx2039400x...
⋮	⋮

ライセンス注入装置 ライセンスDB

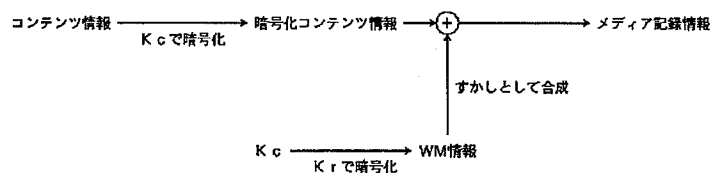
【図122】



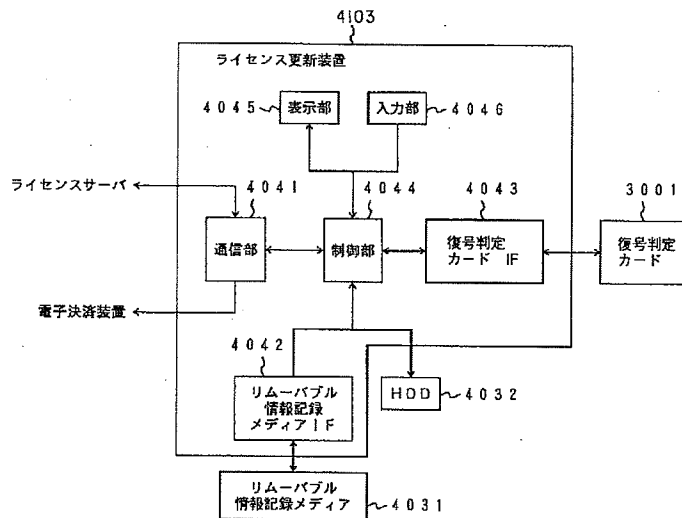
【図151】



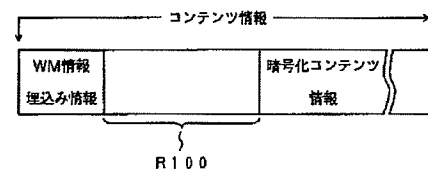
【図166】



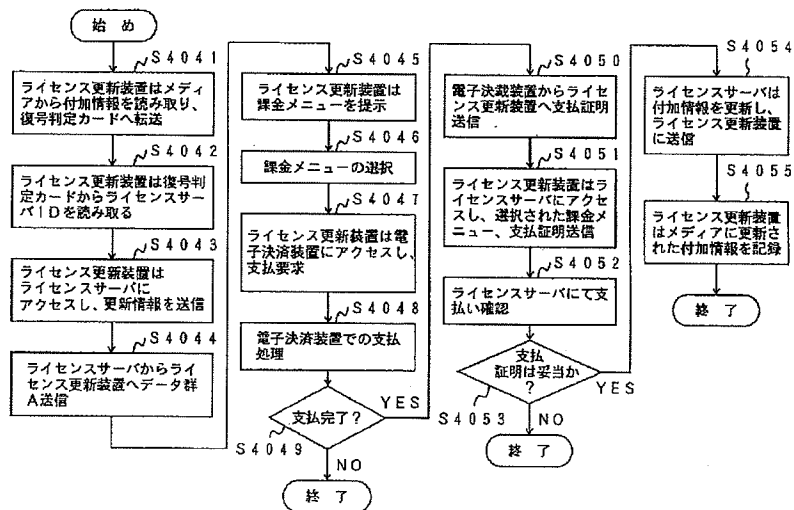
【図104】



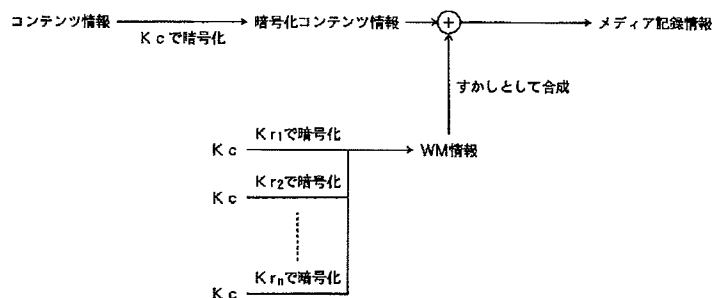
【図172】



【図106】

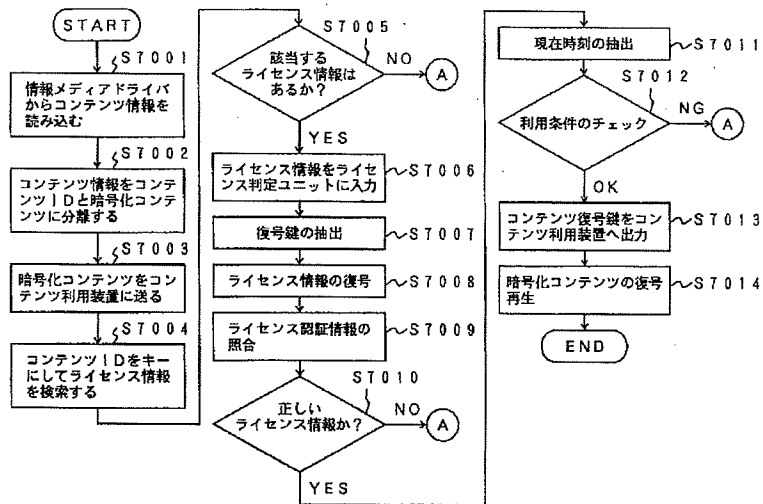


【図170】

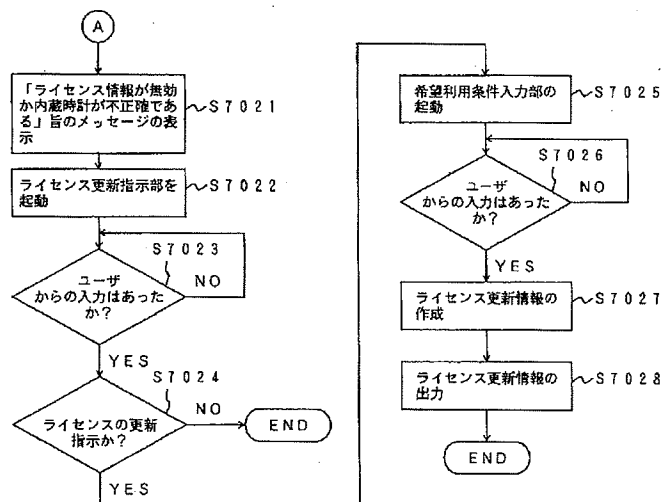


[illegible][illegible]

【図109】

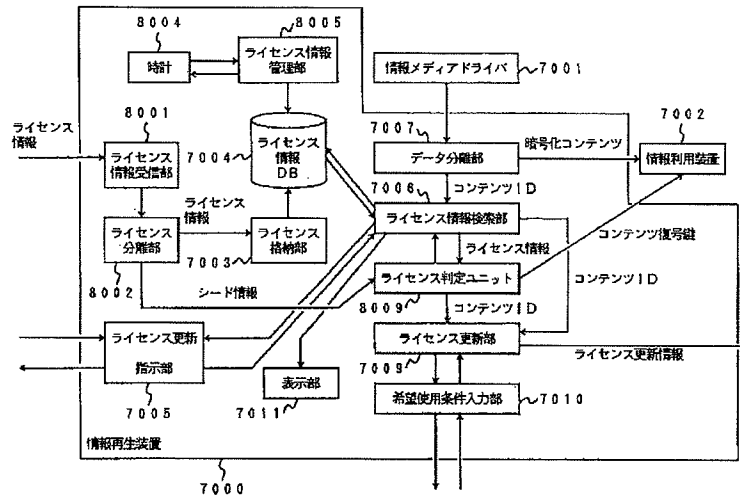


【図110】

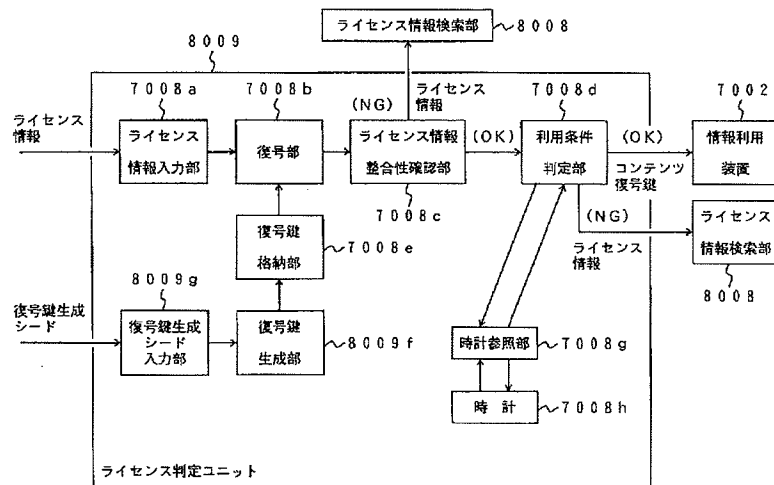




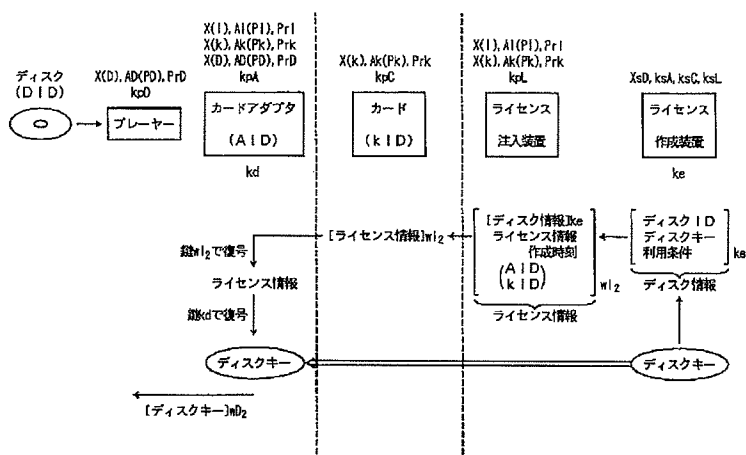
【図118】



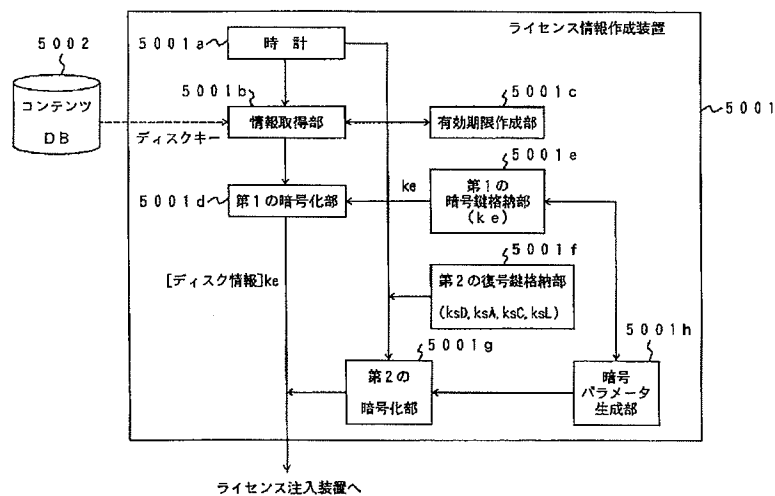
【図 1 1 9】



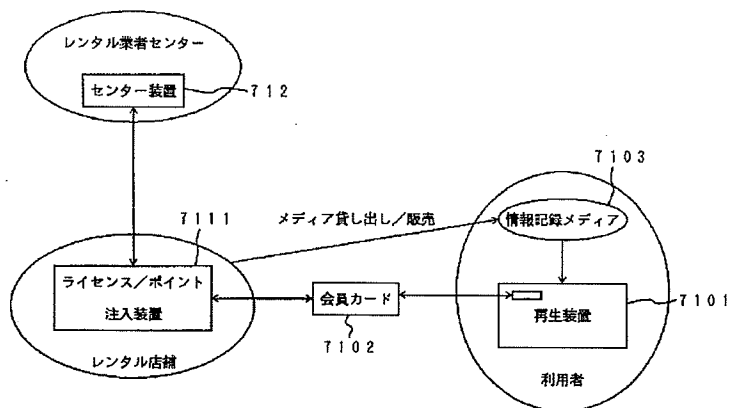
【图125】



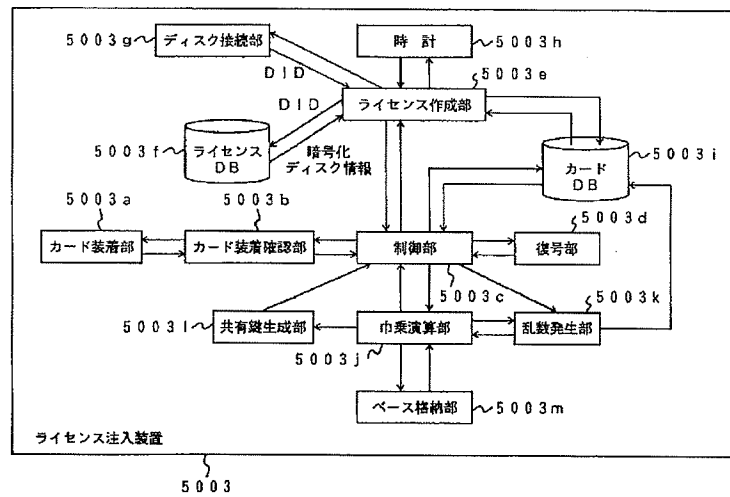
【图 126】



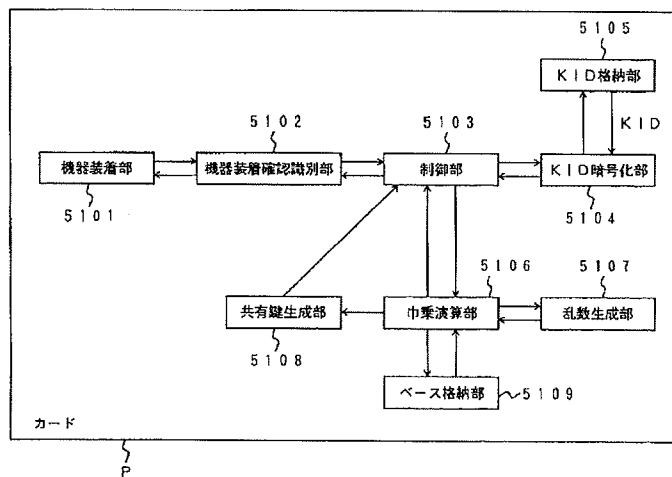
【図 150】



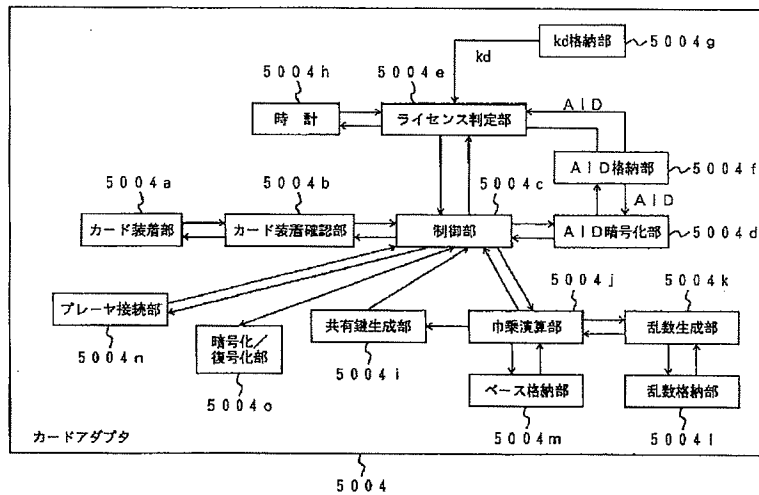
【図127】



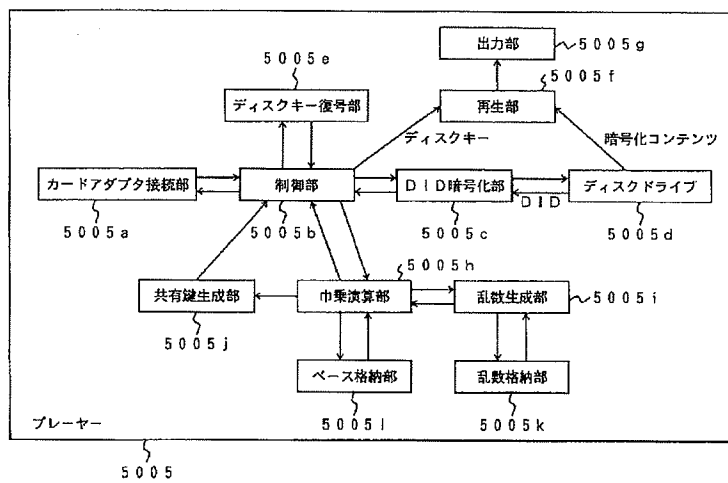
【図128】



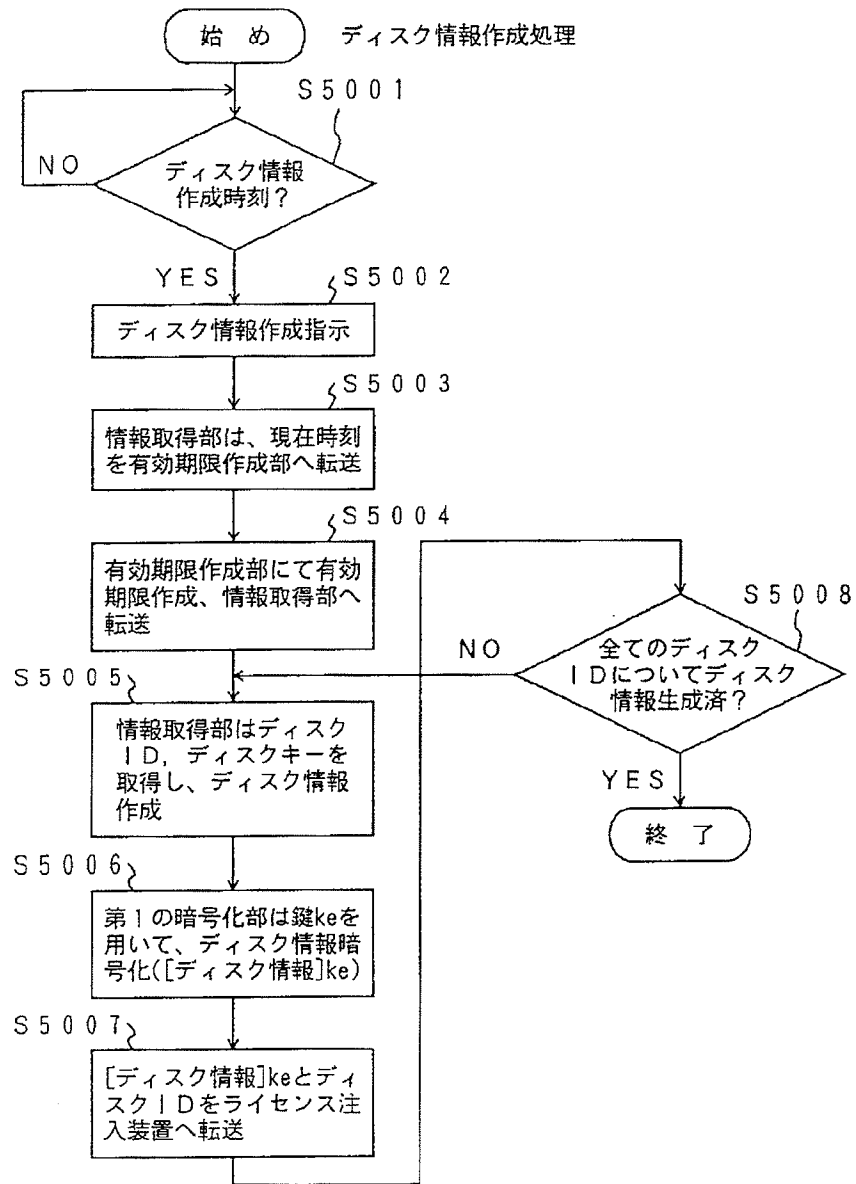
【図129】



【図130】

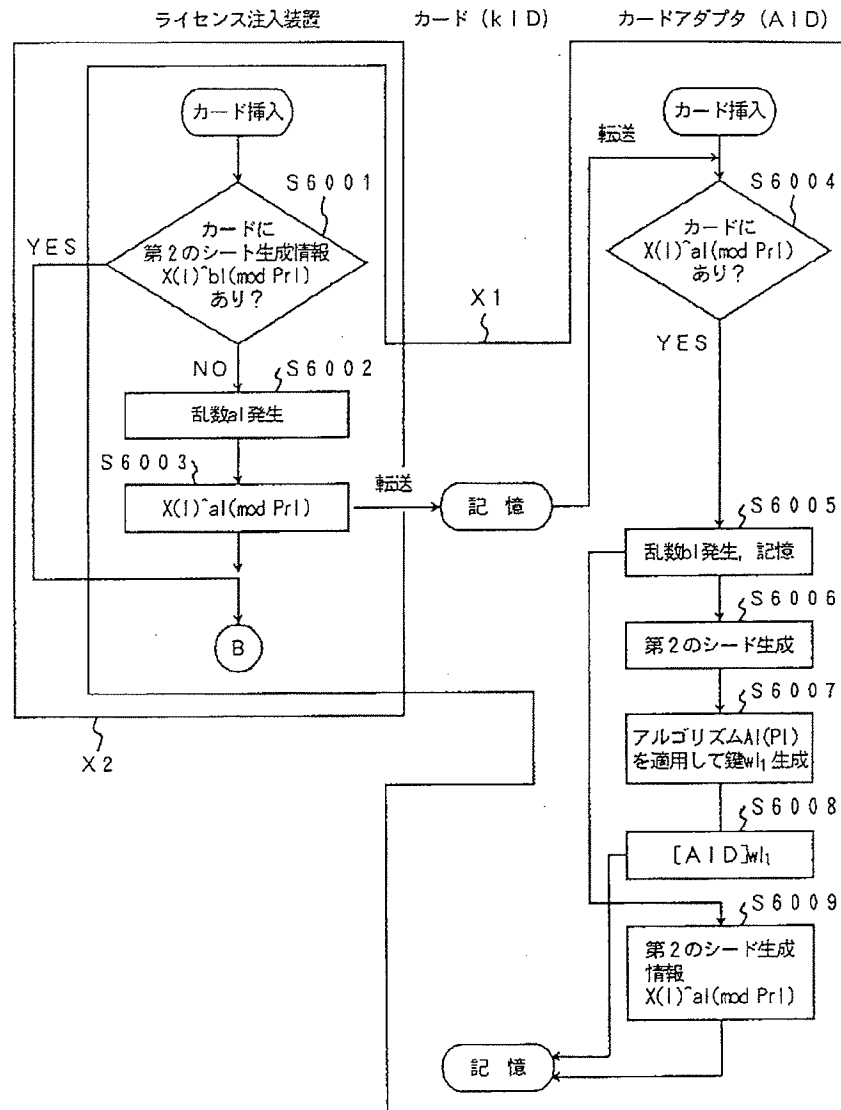


【図131】

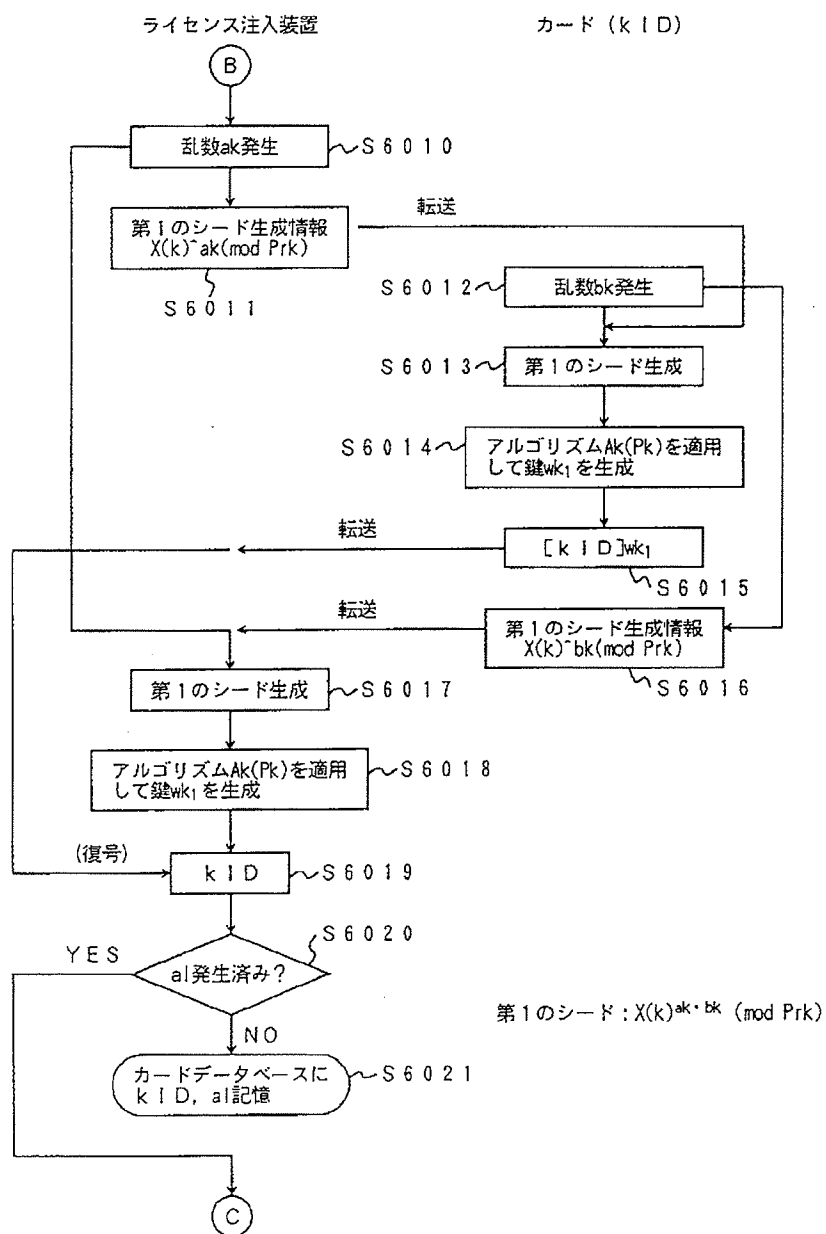




【図134】

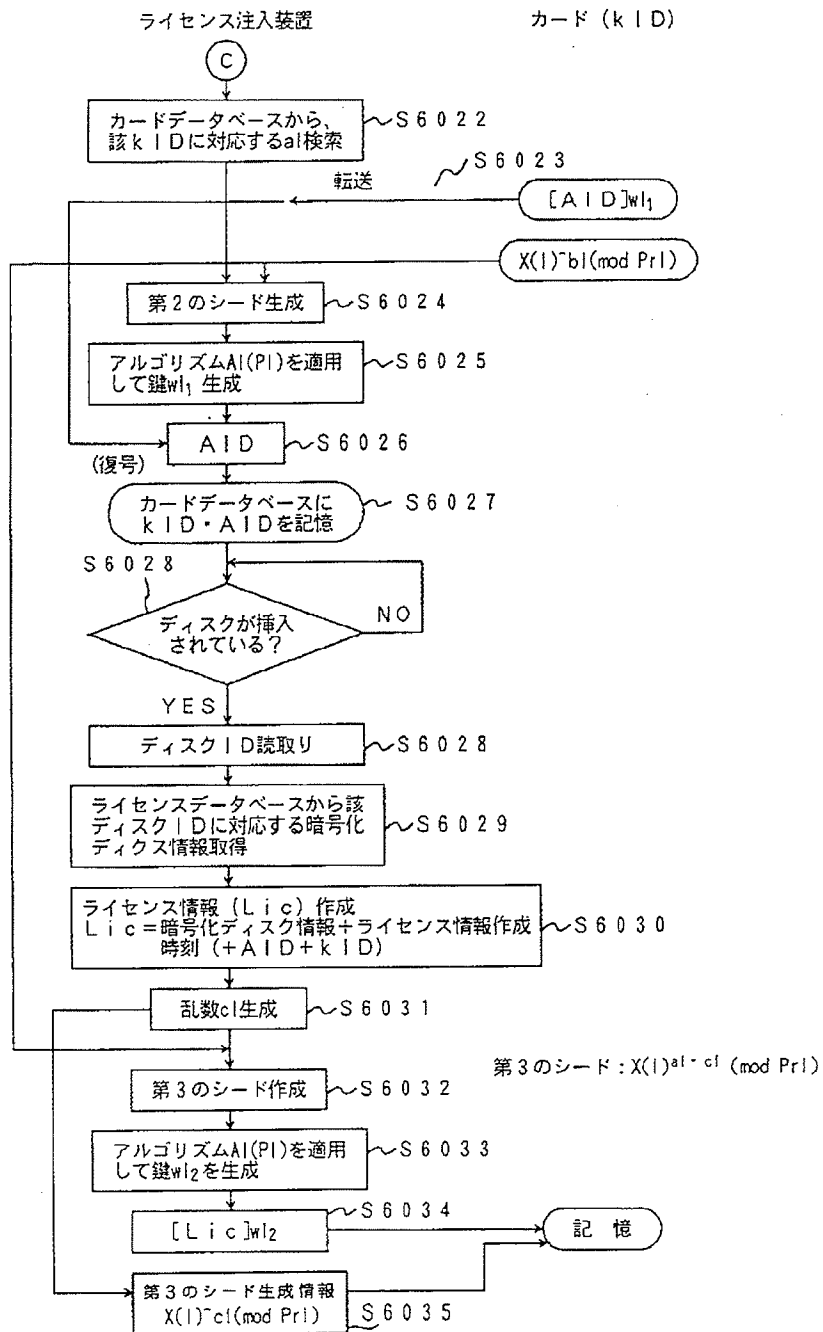
第2のシード:  $X(1)^{a1 \cdot bl(mod Pr1)}$

【图135】

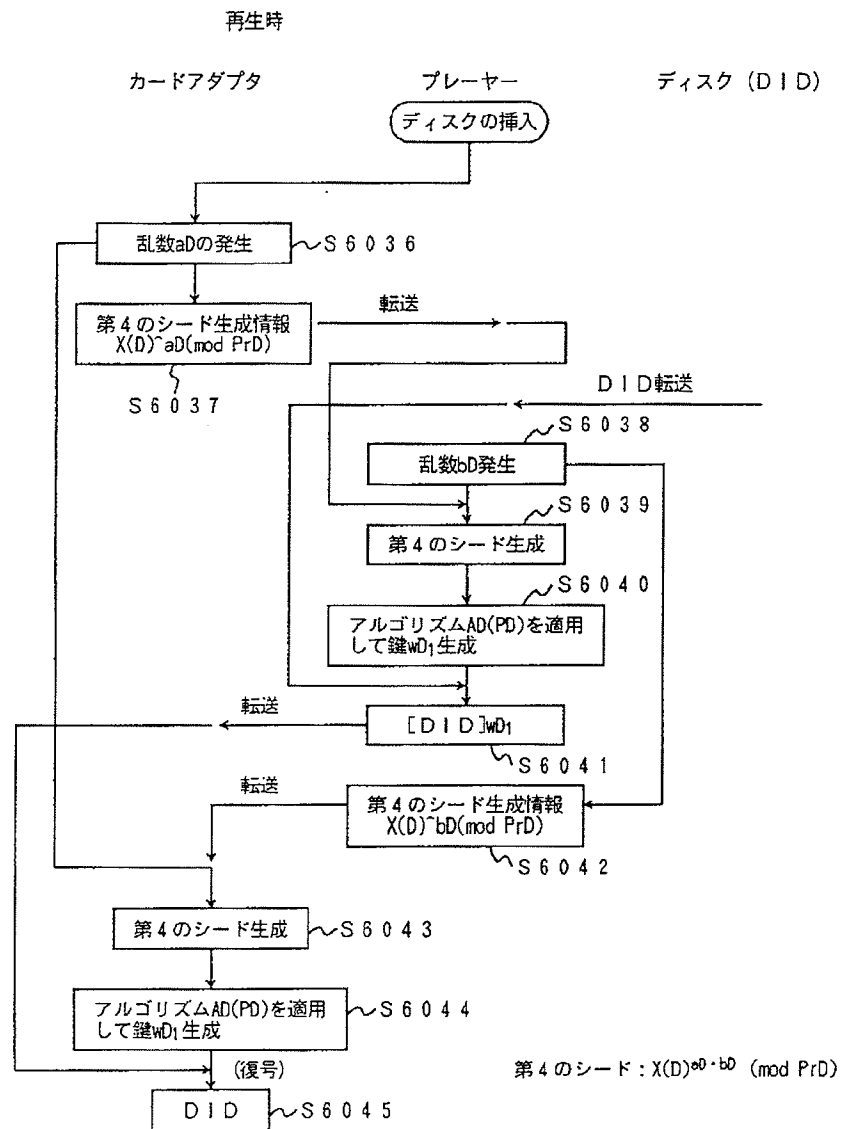




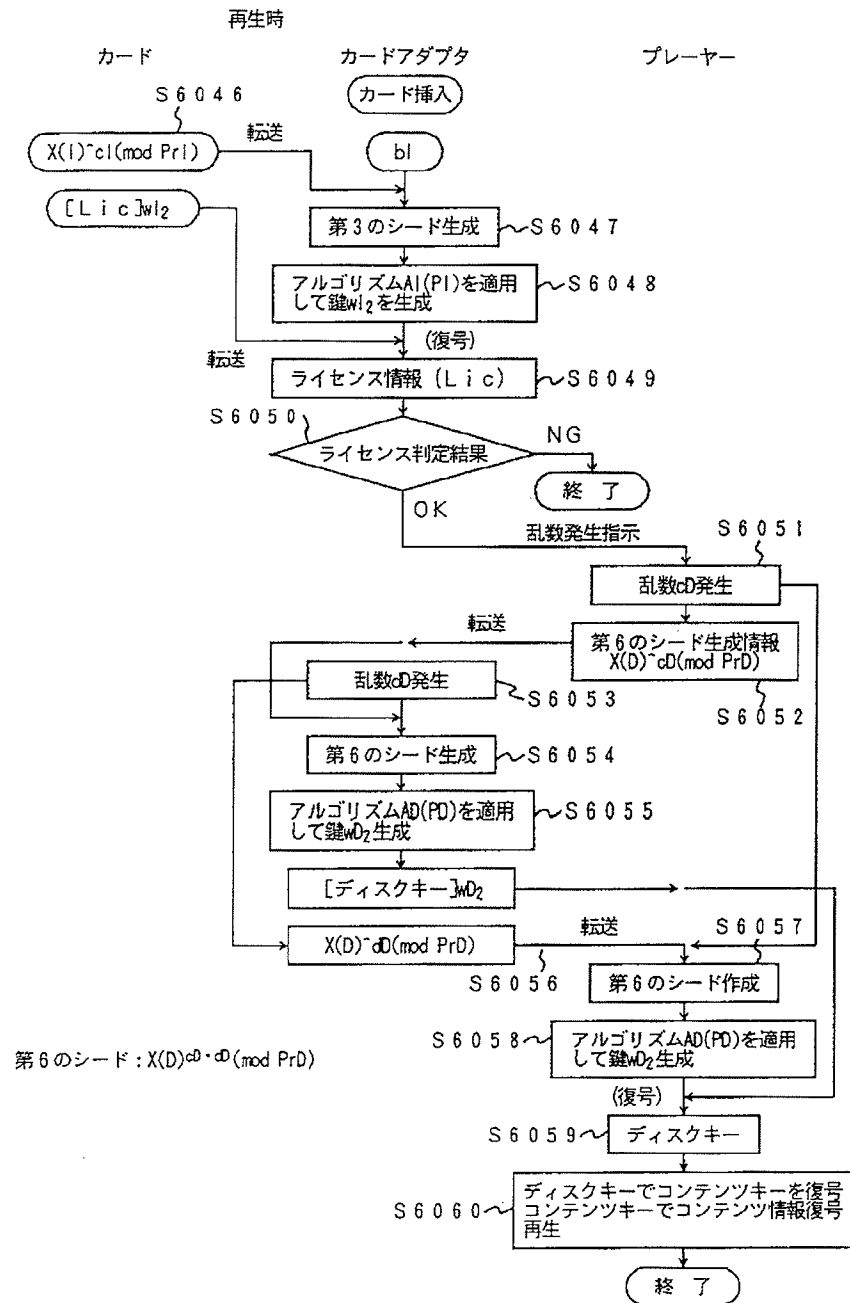
【図136】



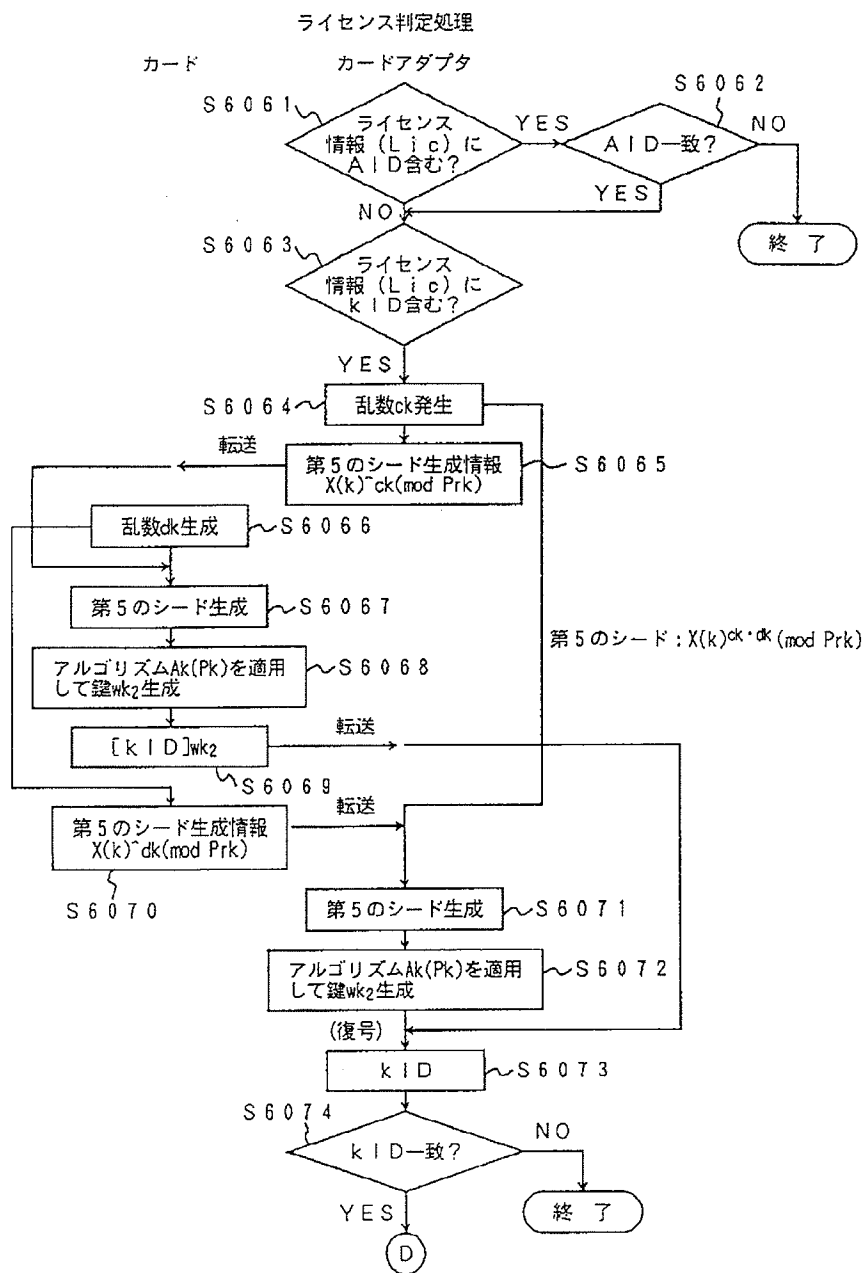
【図137】



【図138】

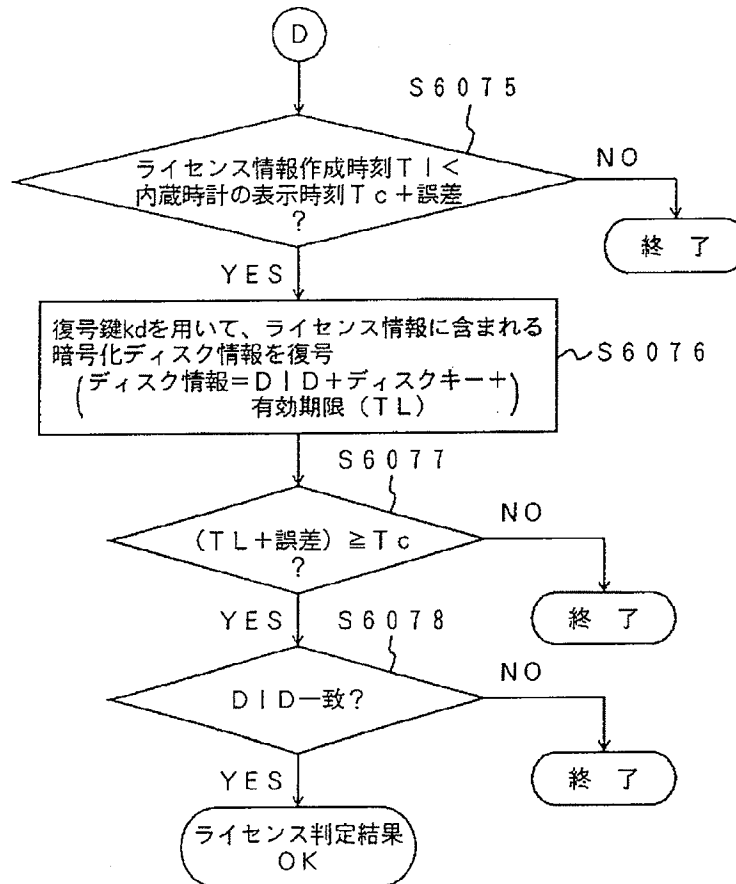


【図139】

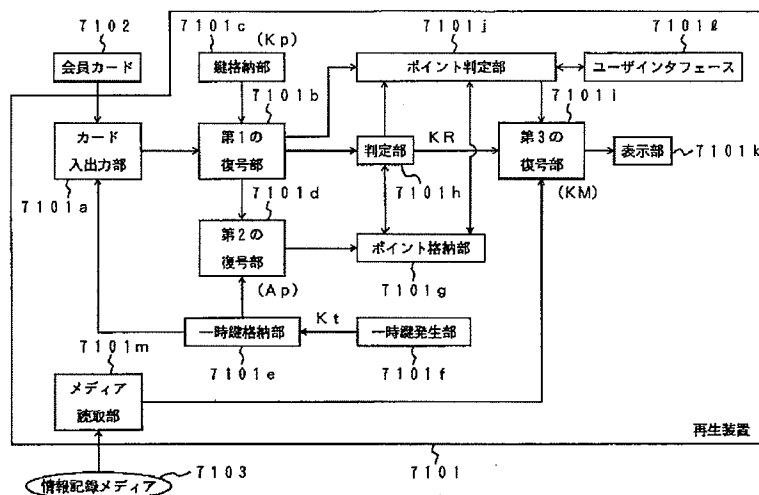


【図140】

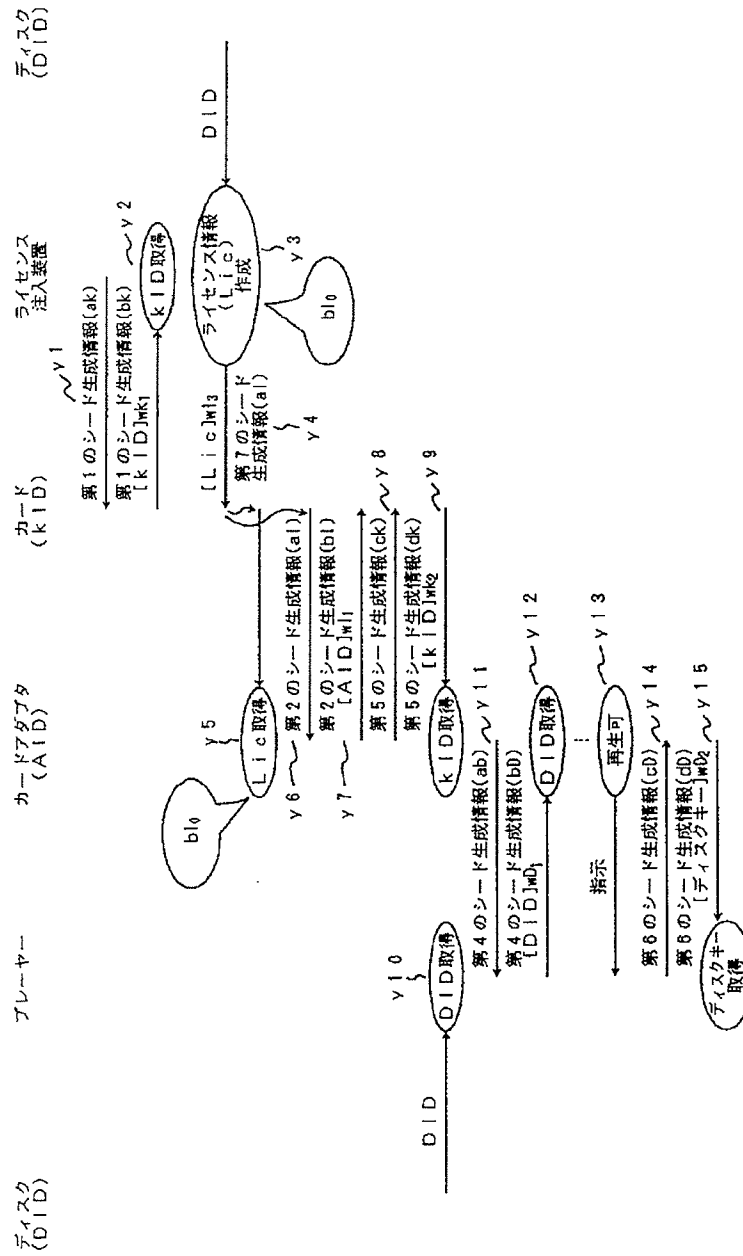
カードアダプタ



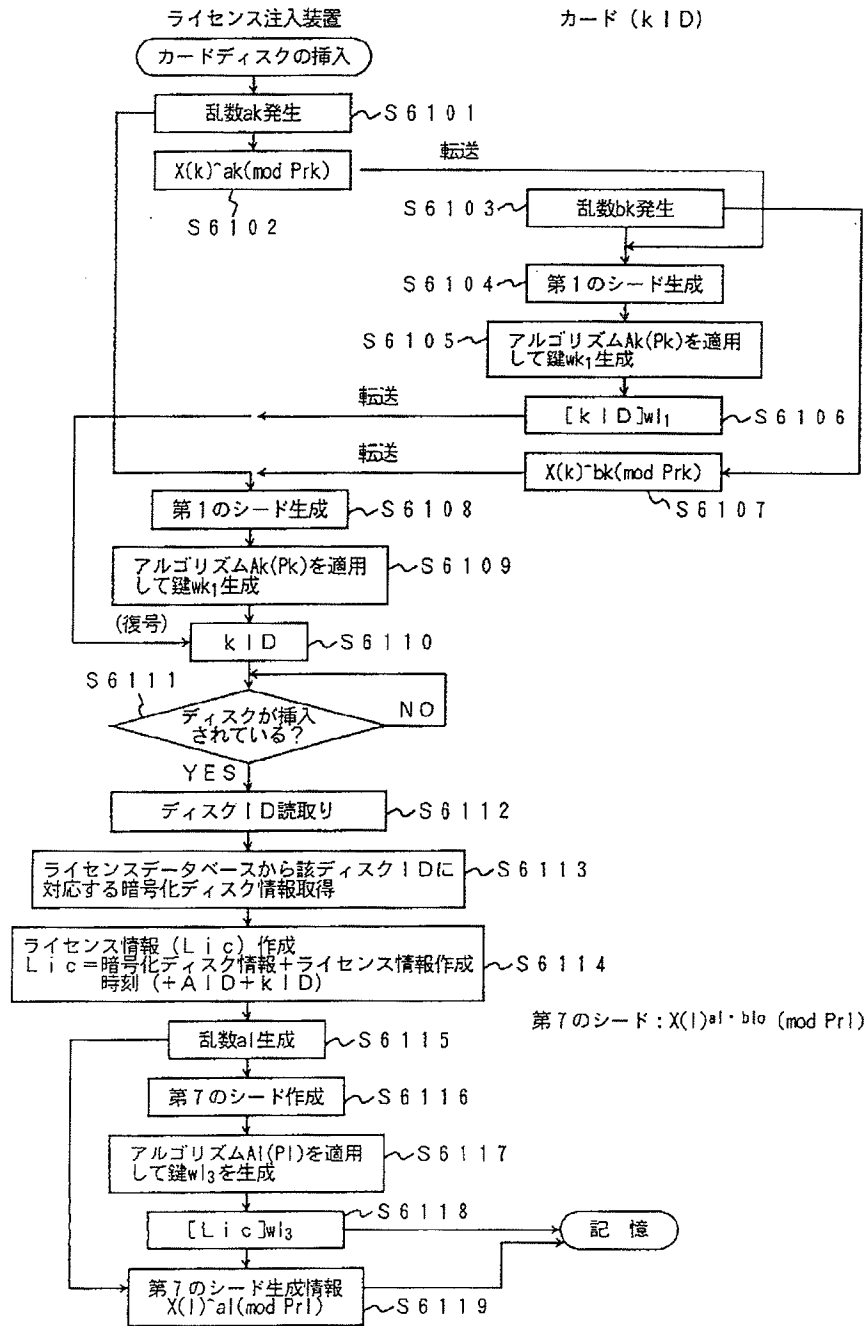
【図152】



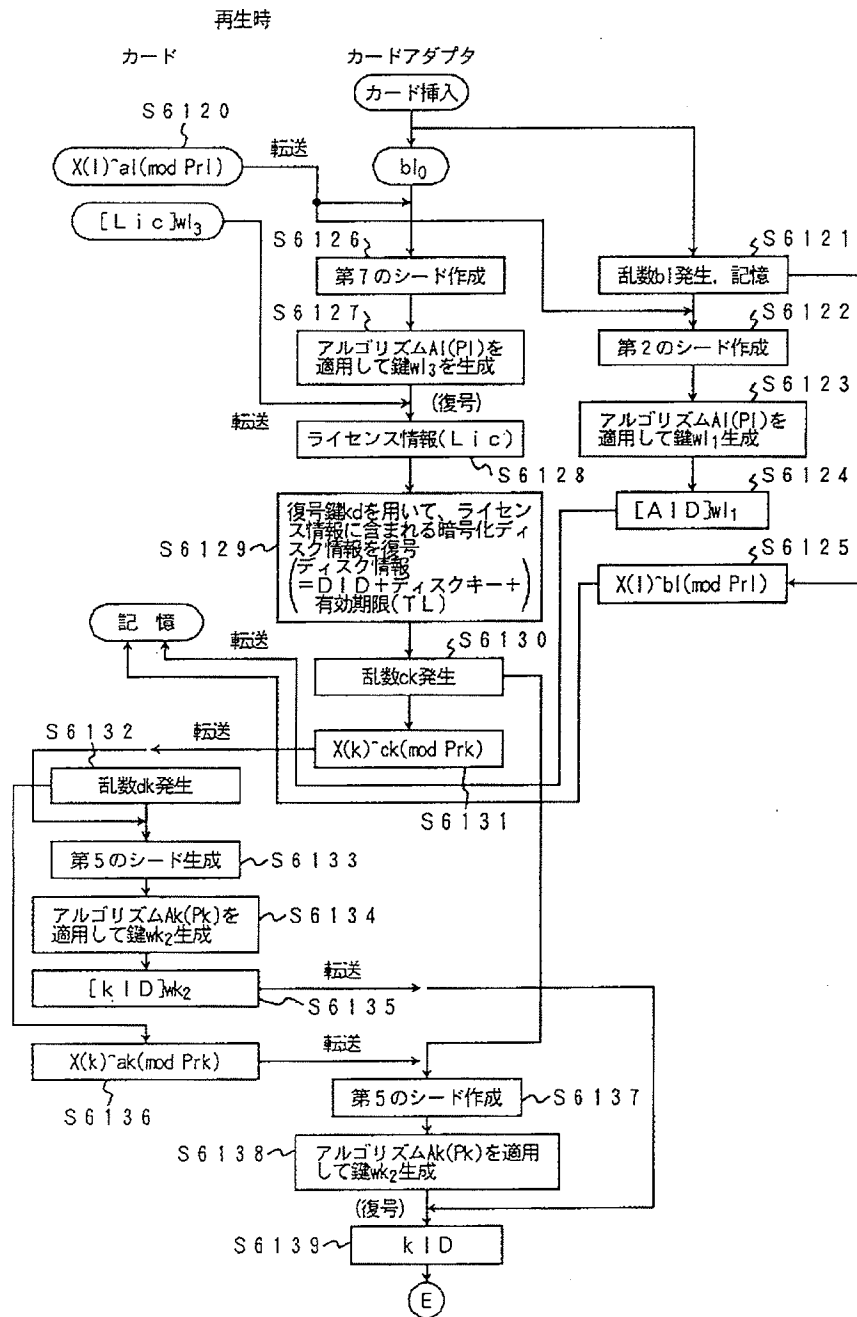
【図141】



【図142】

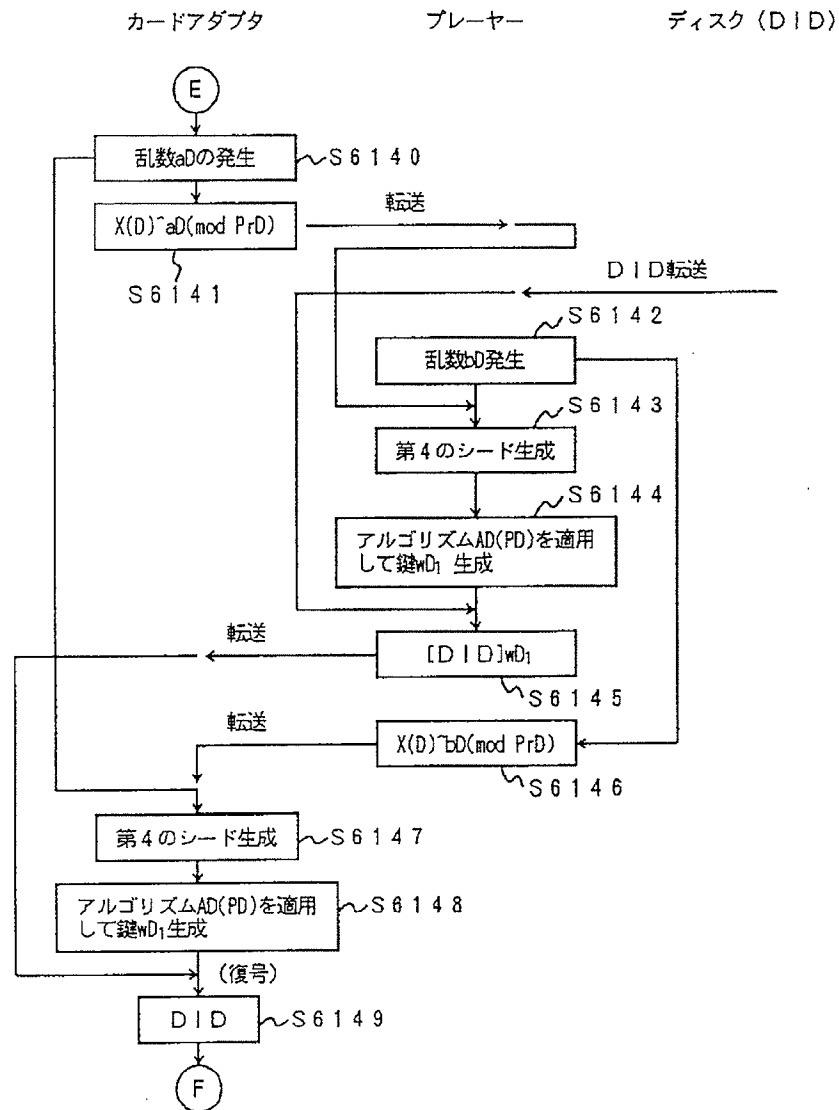


【図143】

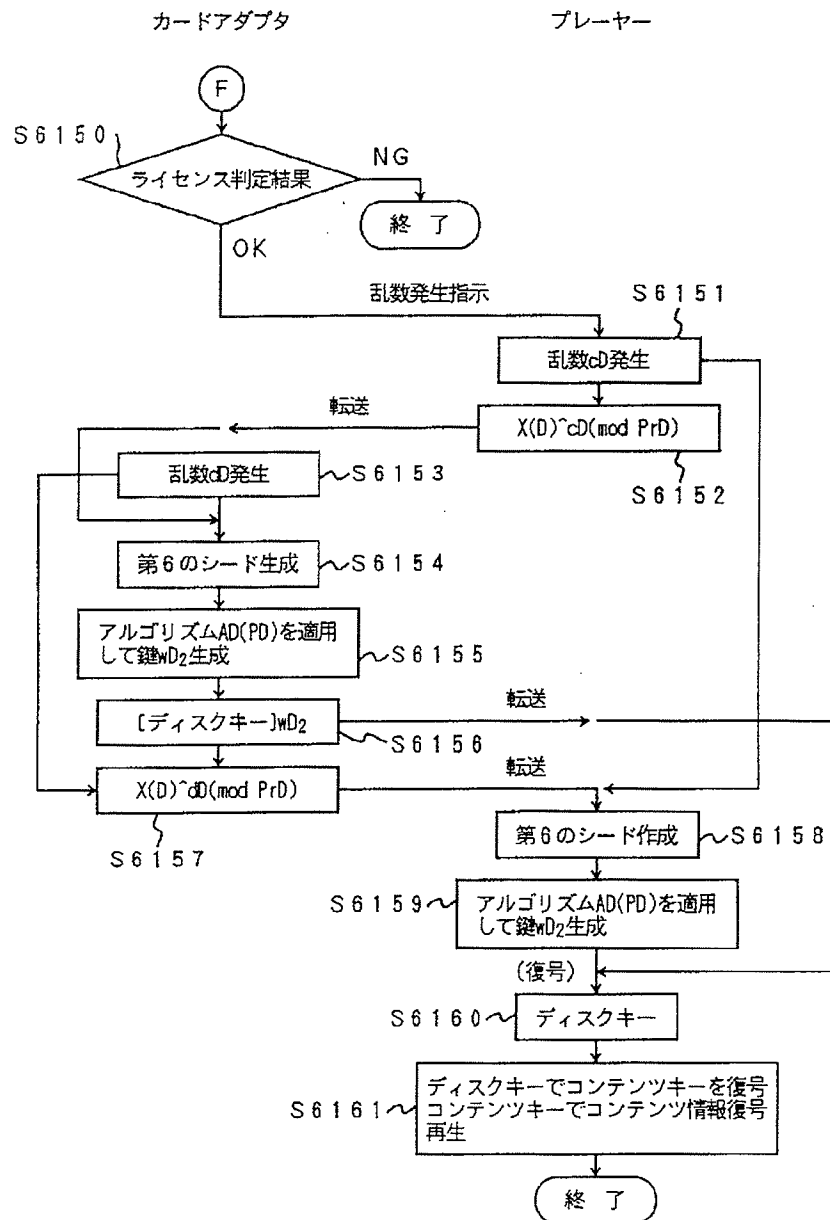




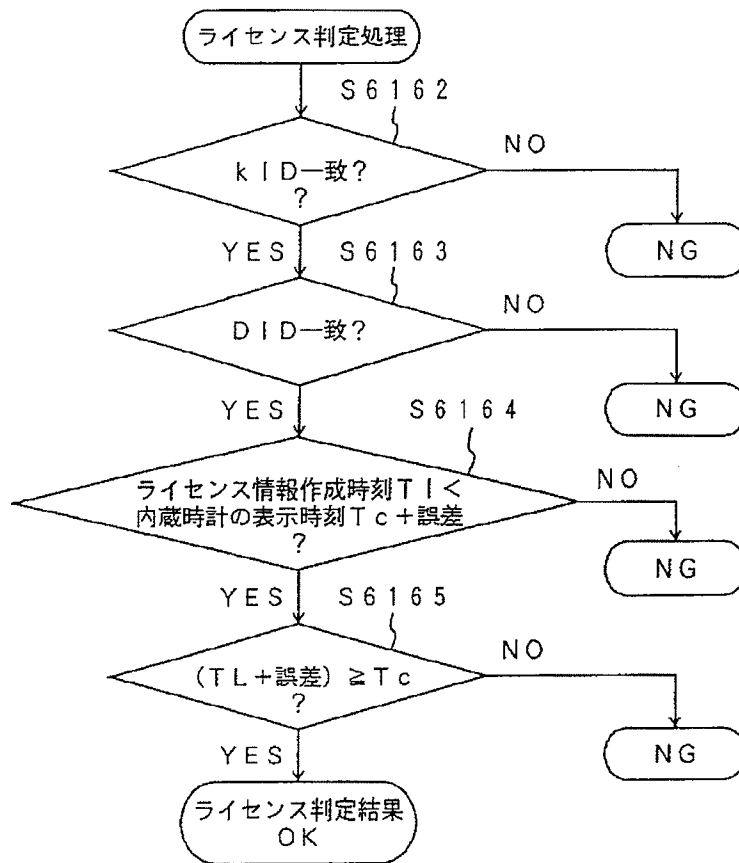
【図144】



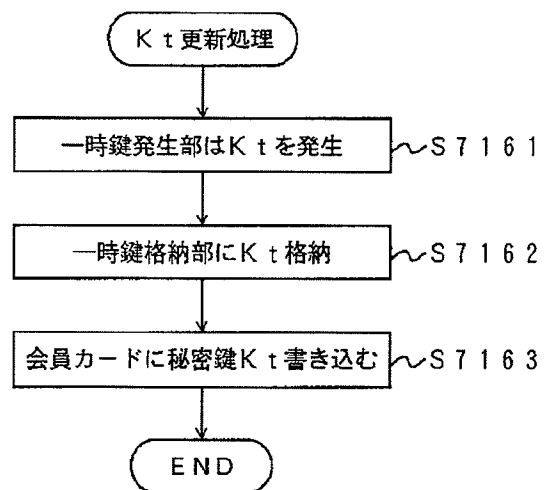
【図145】



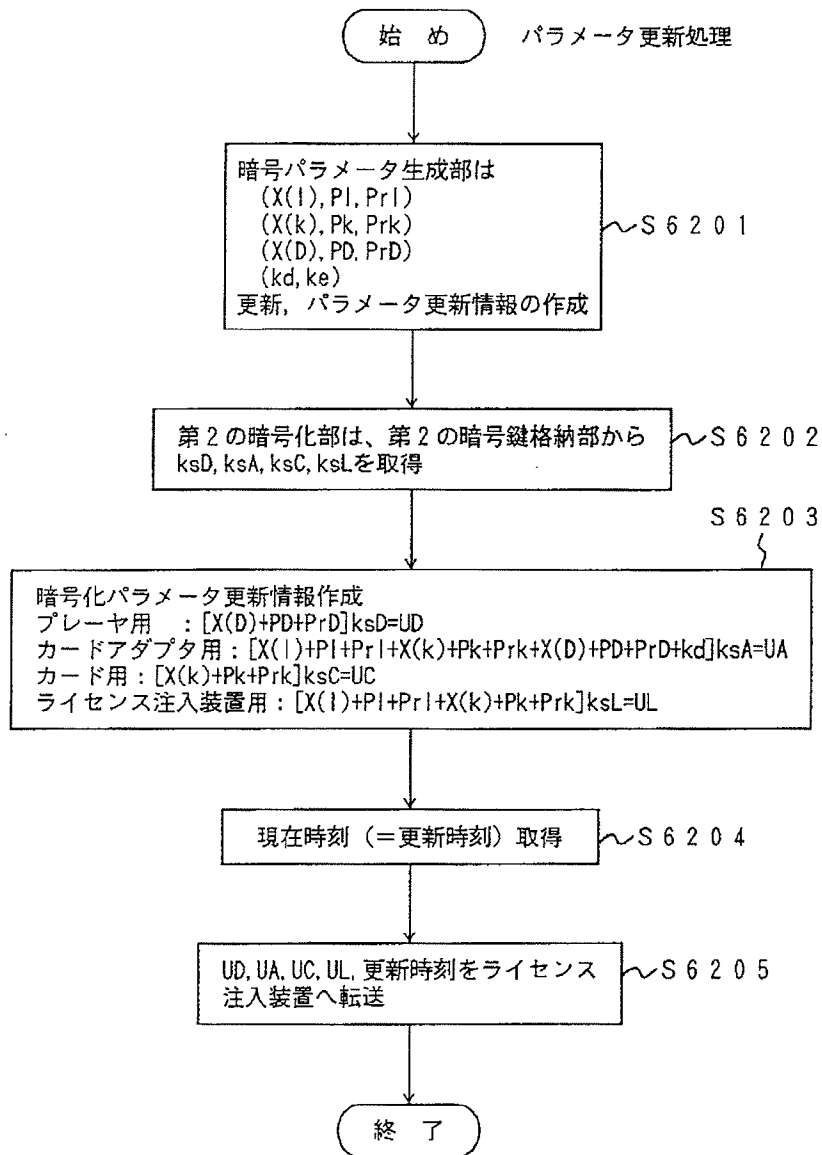
【図146】



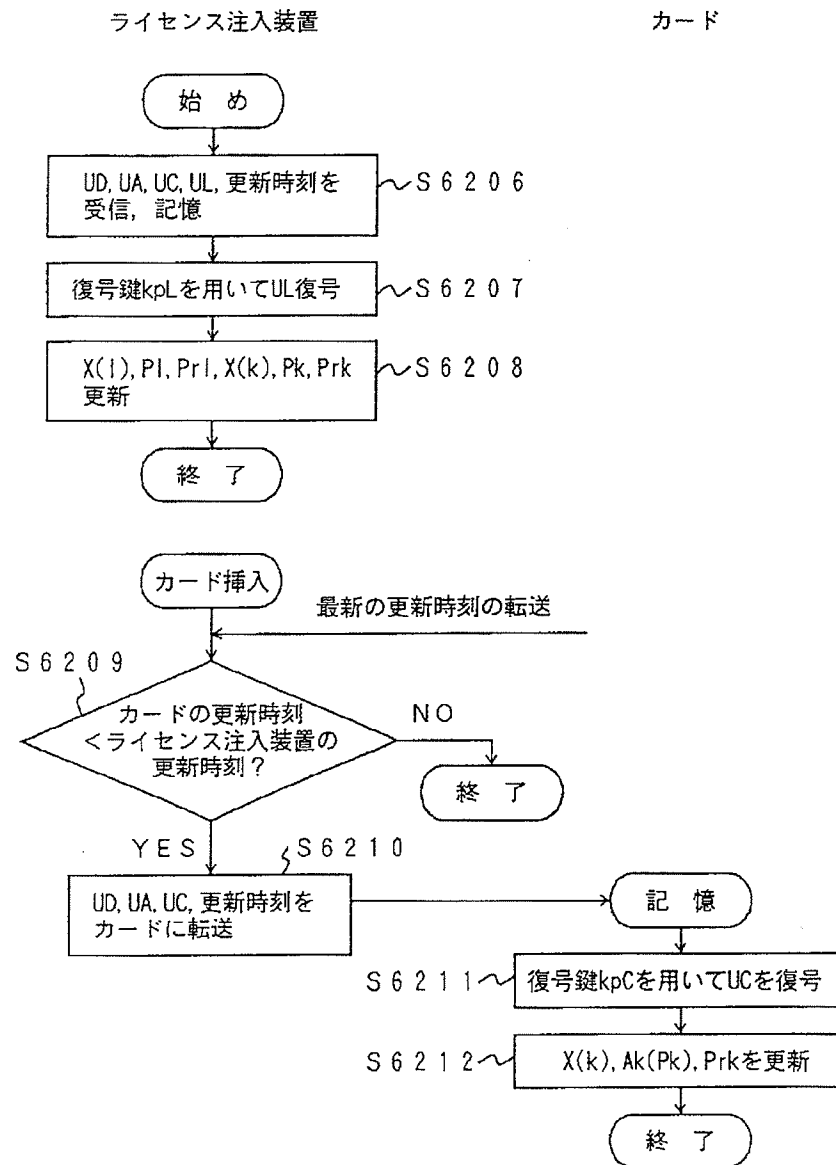
【図158】



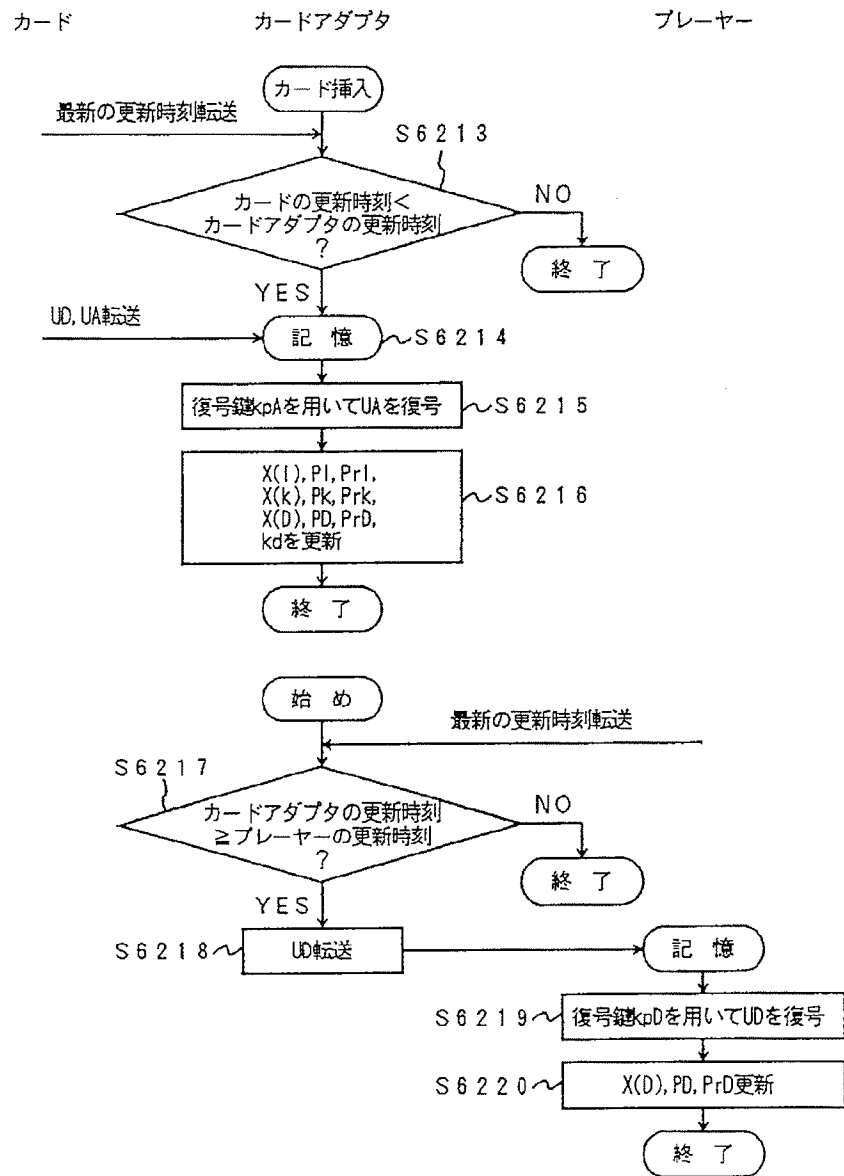
【図147】



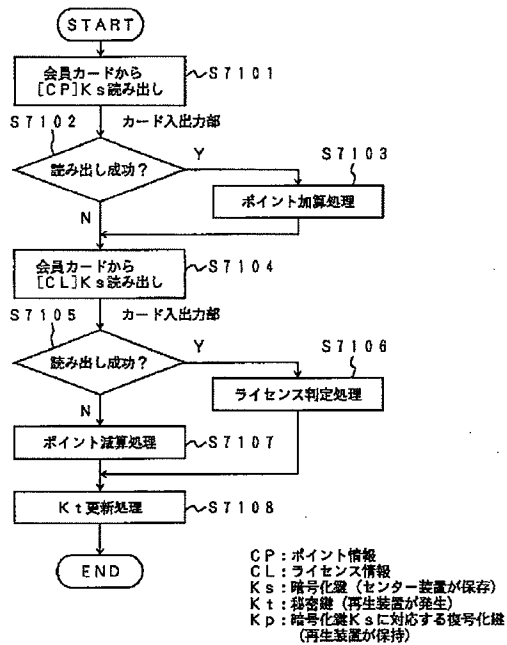
【図148】



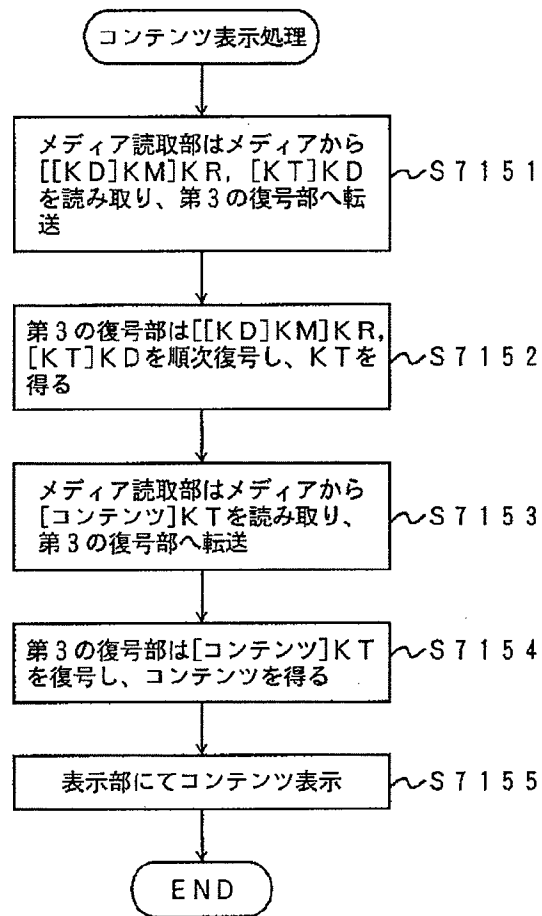
【図149】



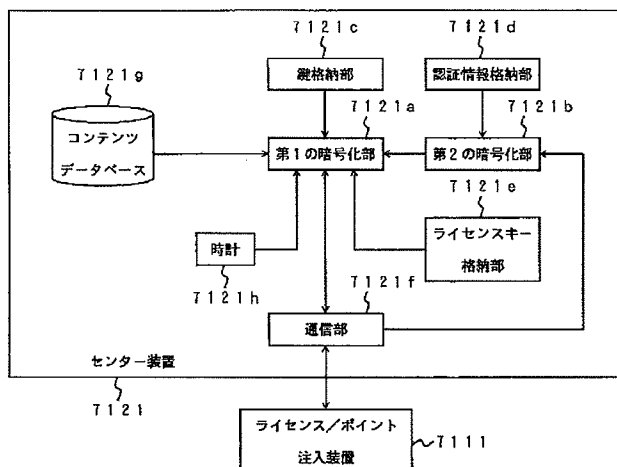
【図153】



【図157】



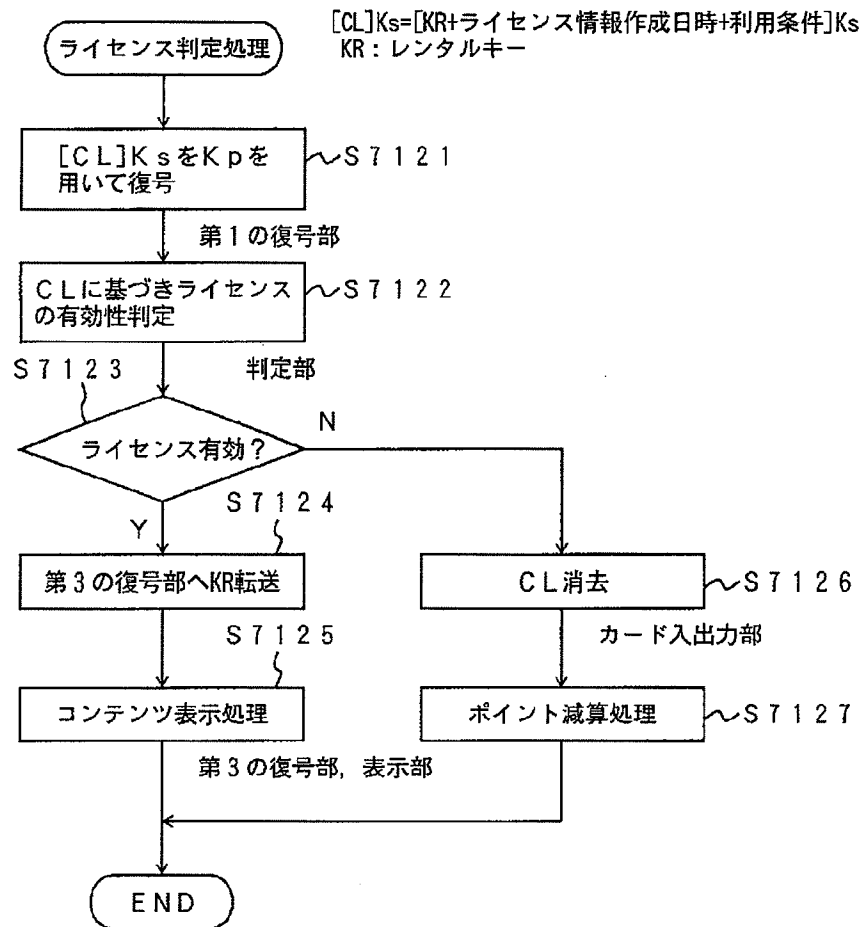
【図162】



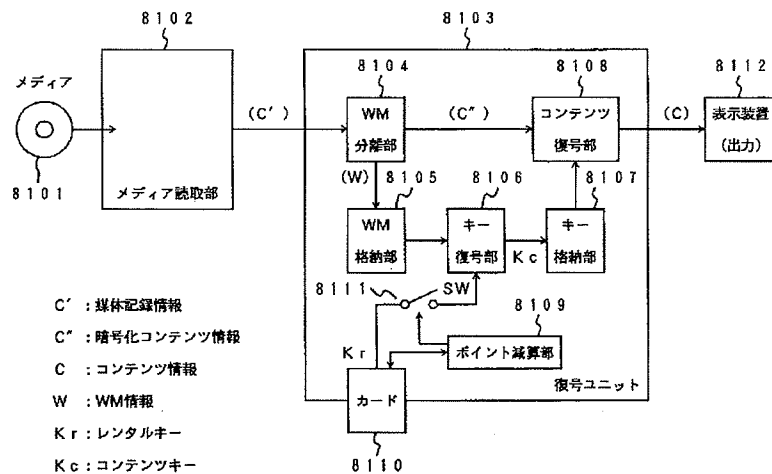




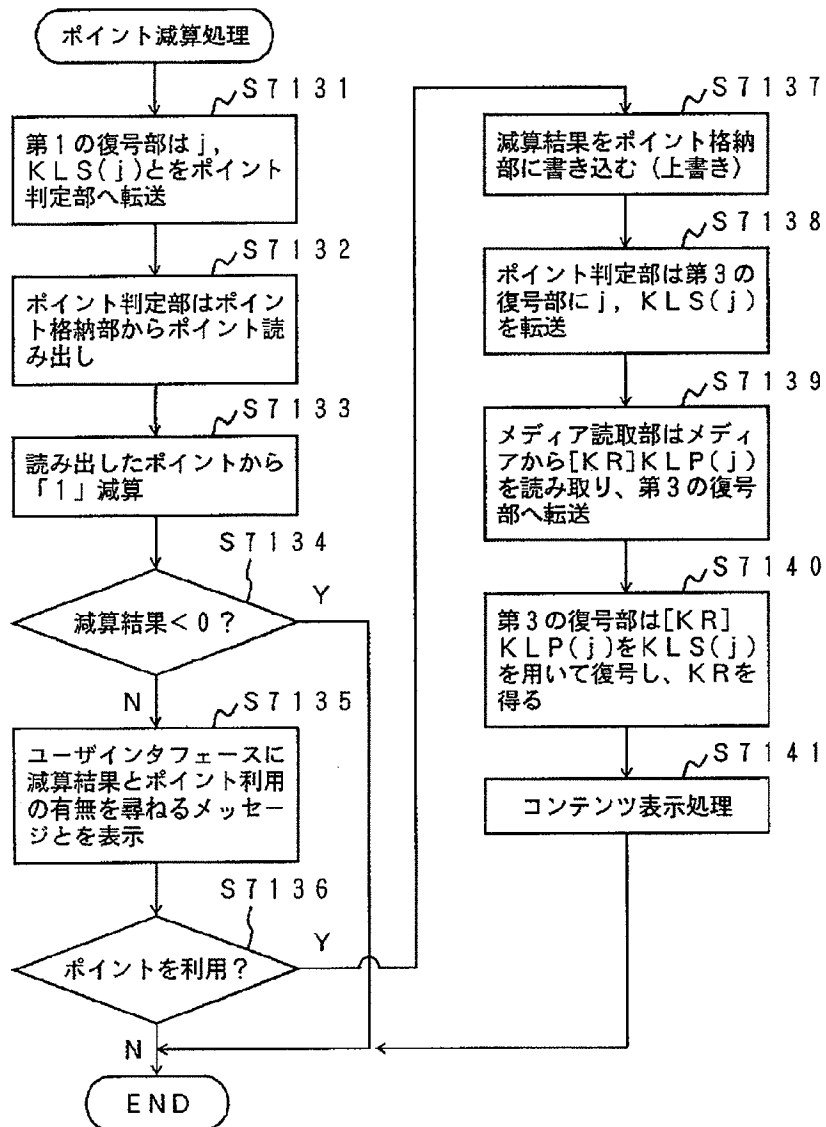
【図155】



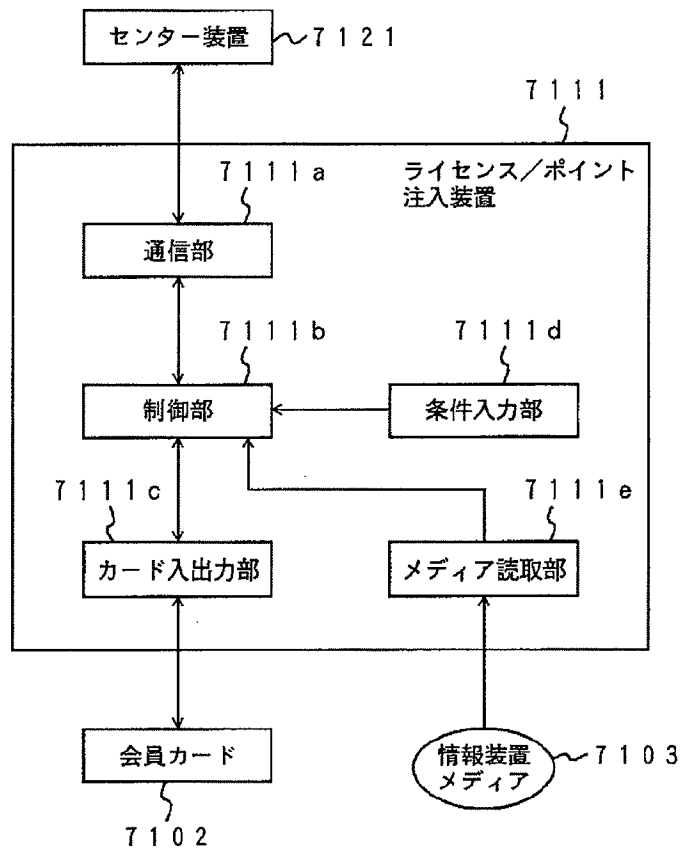
【図165】



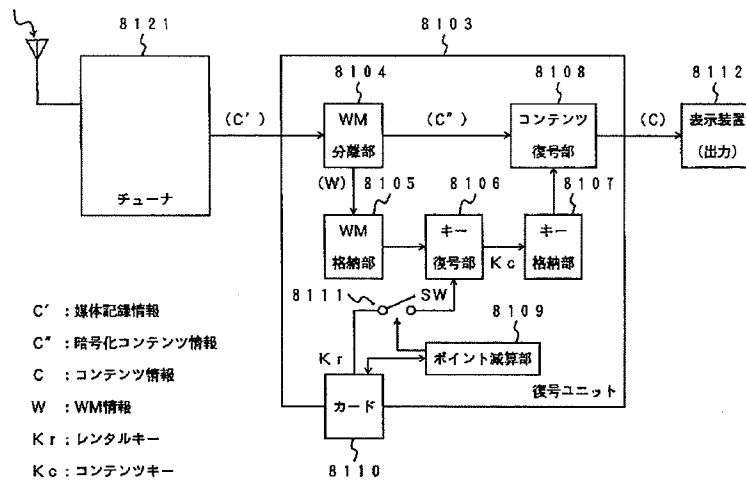
【図156】



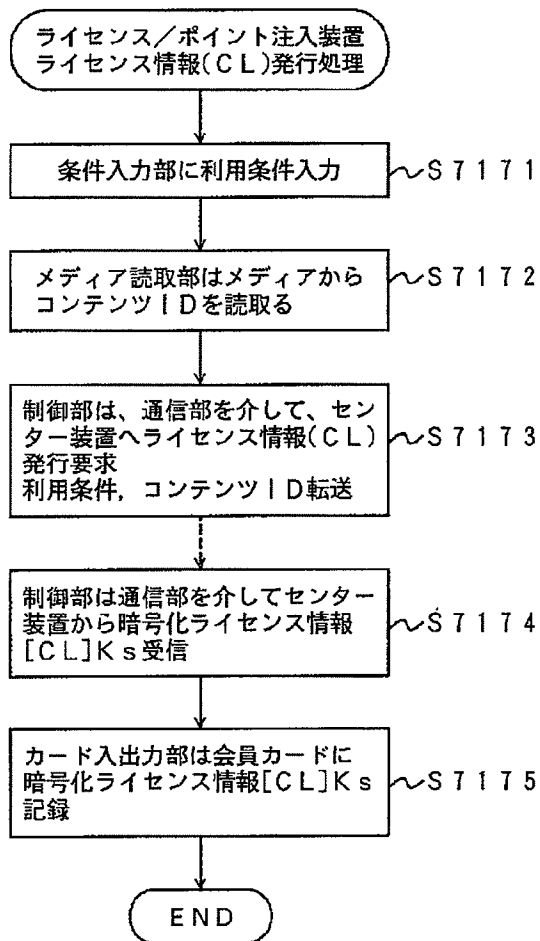
【図159】



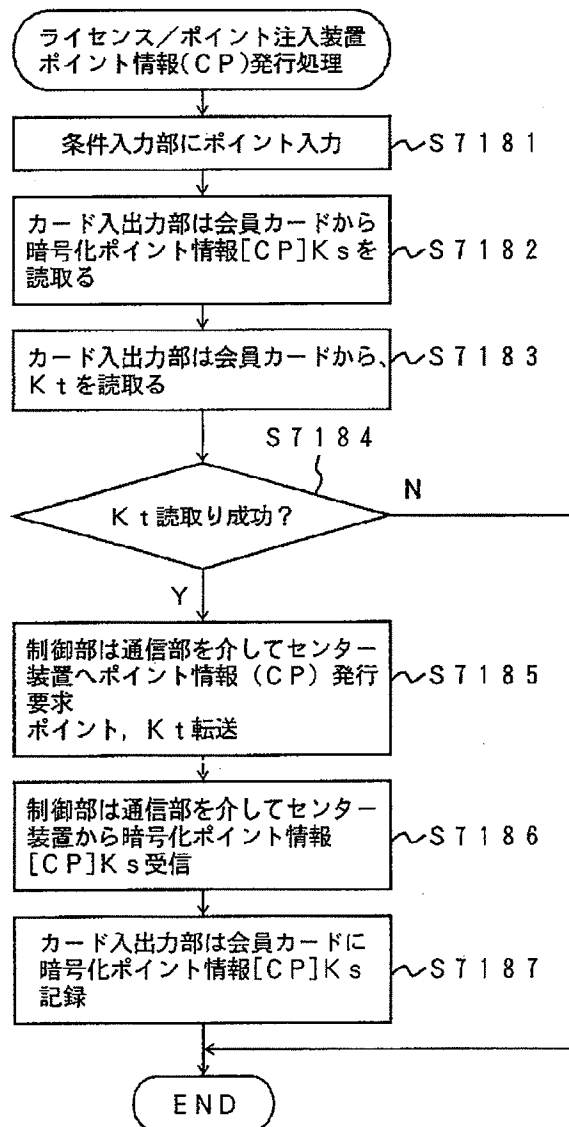
【図168】



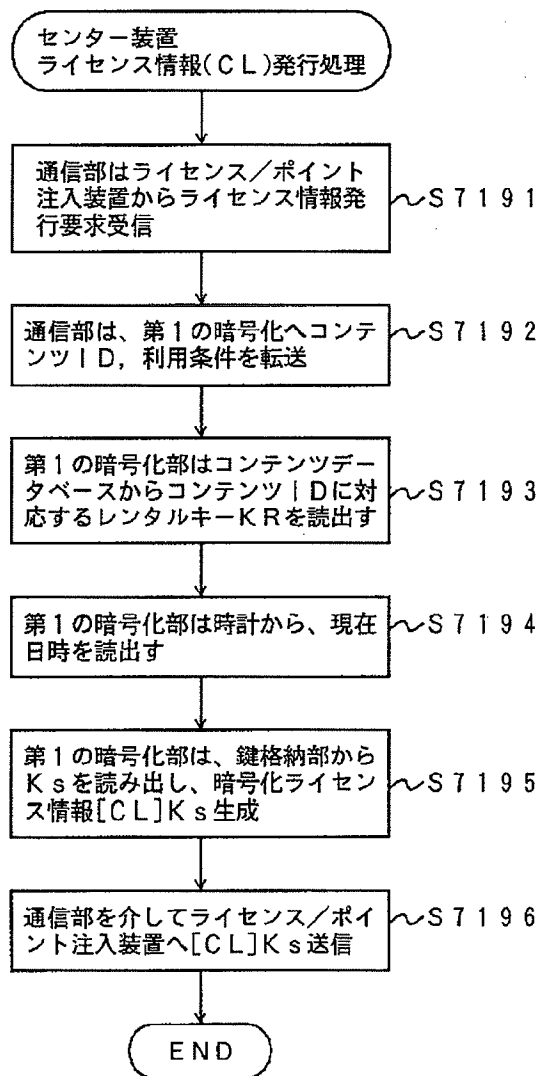
【図160】



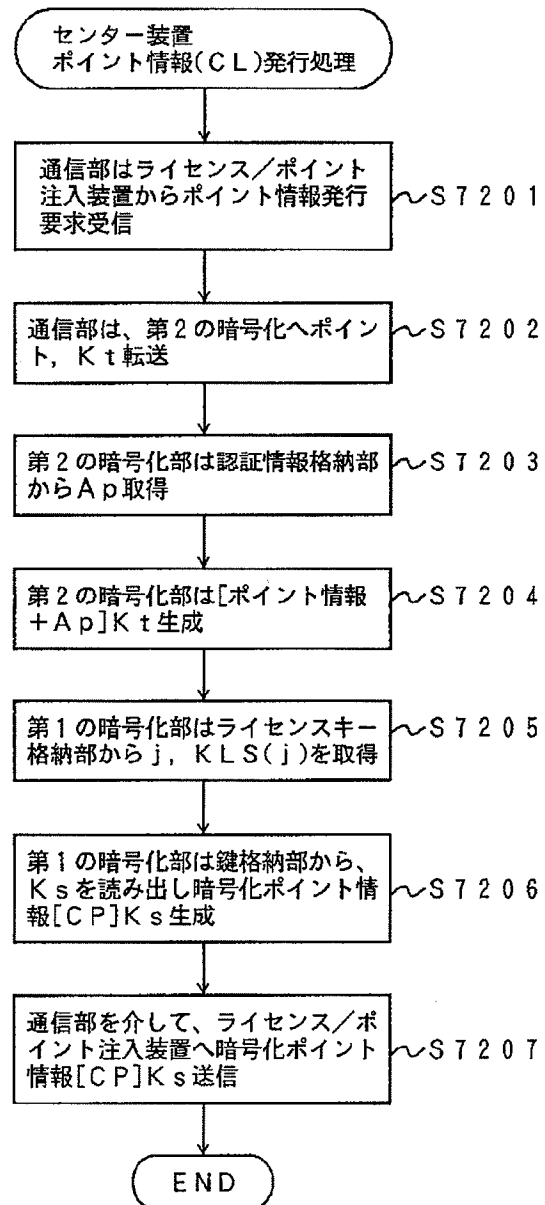
【図161】



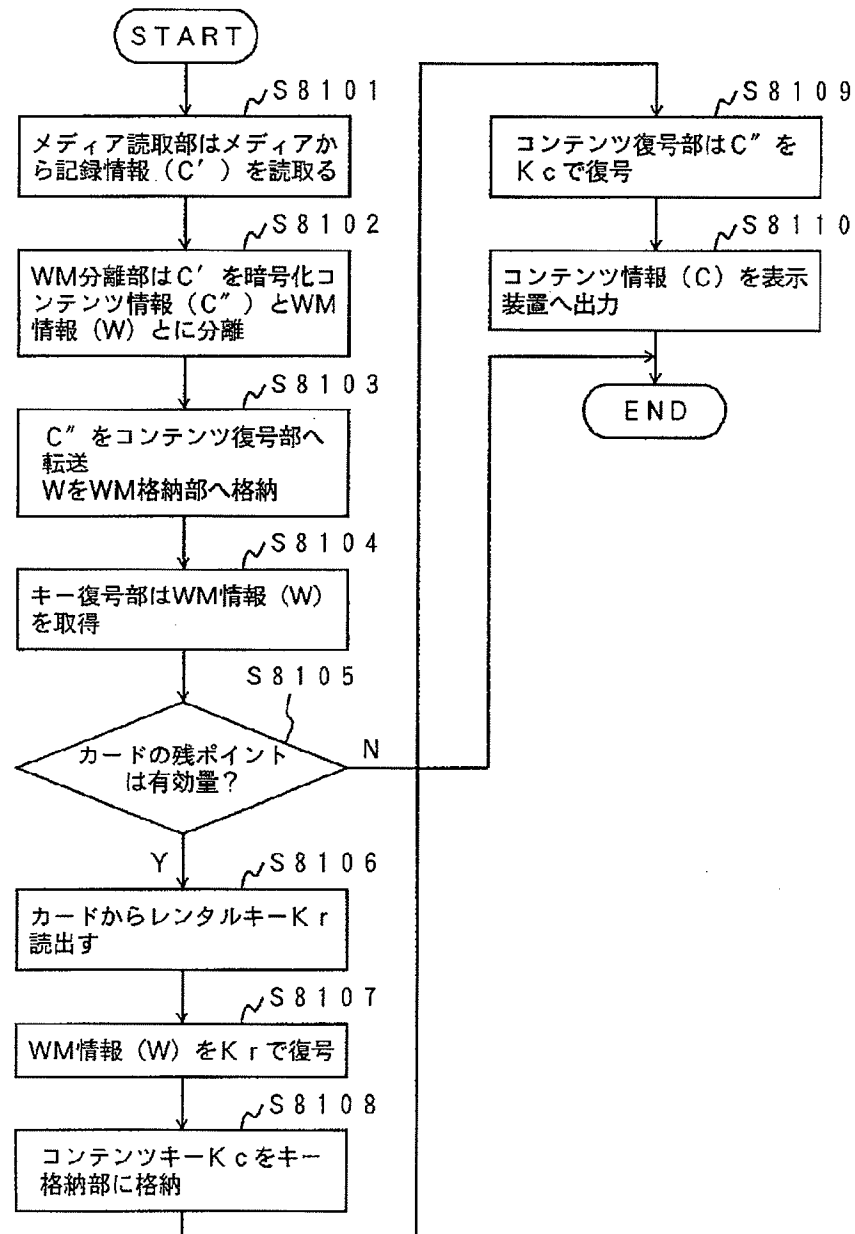
【図163】



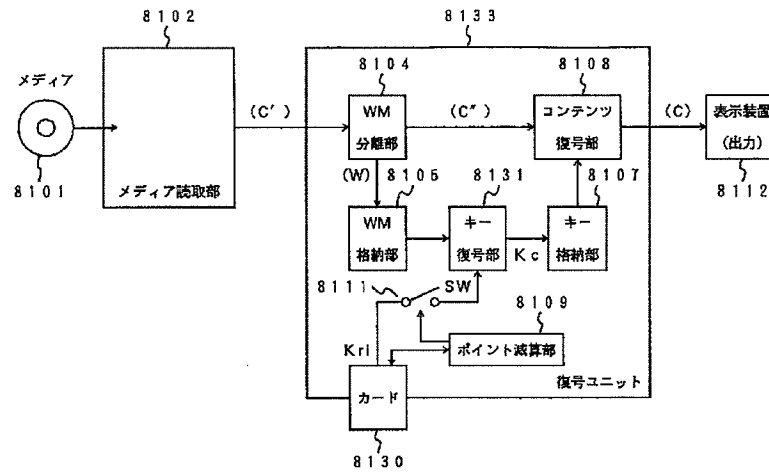
【図164】



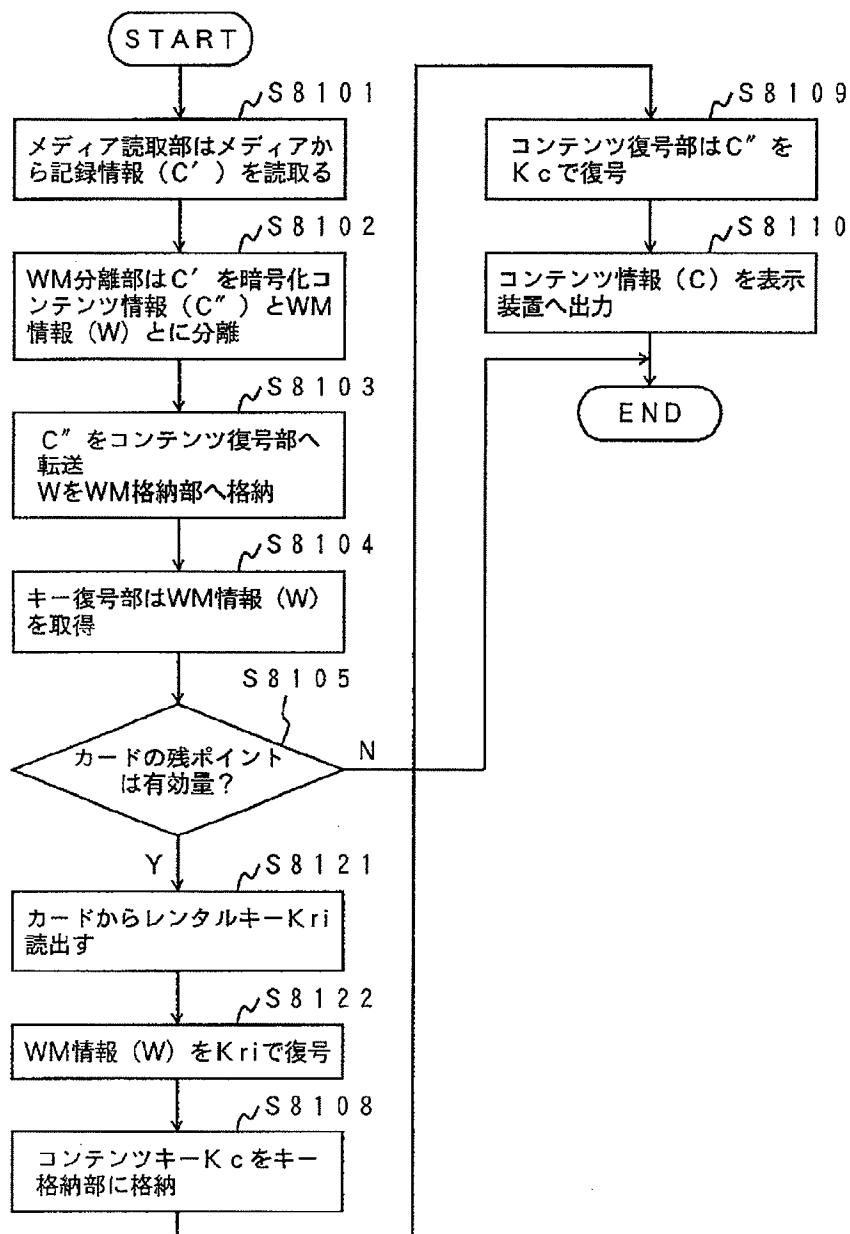
【図167】



【図169】



【図171】



【手続補正書】

【提出日】平成10年7月3日

【手続補正1】

【補正対象書類名】図面

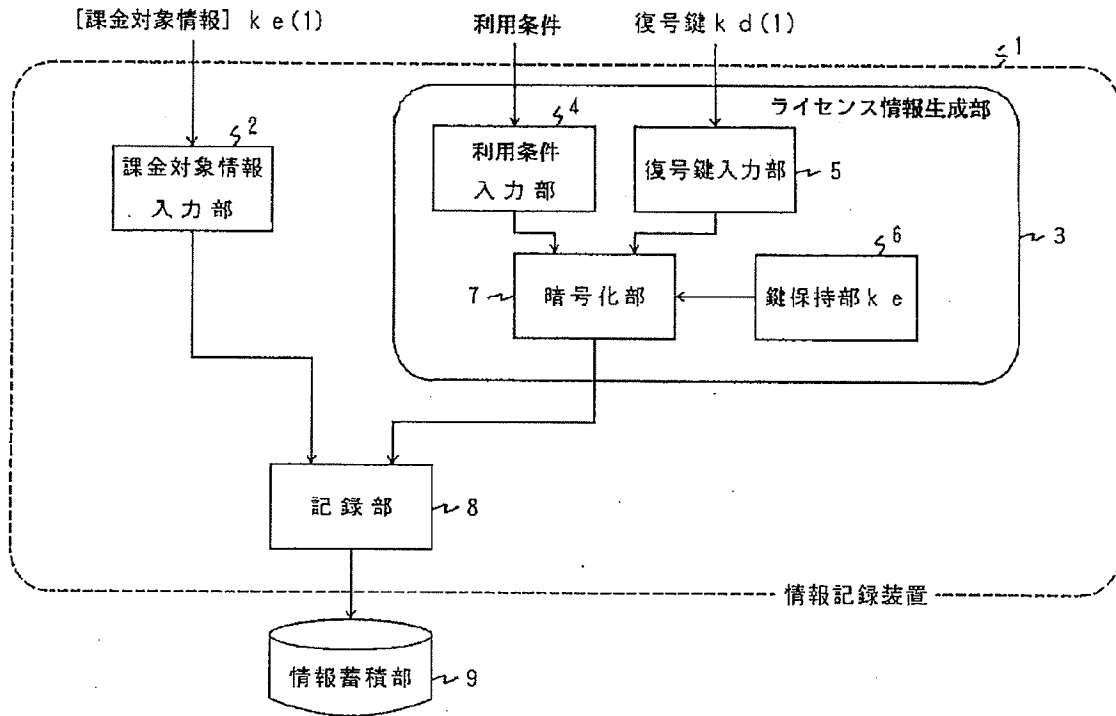
【補正対象項目名】全図

【補正方法】変更

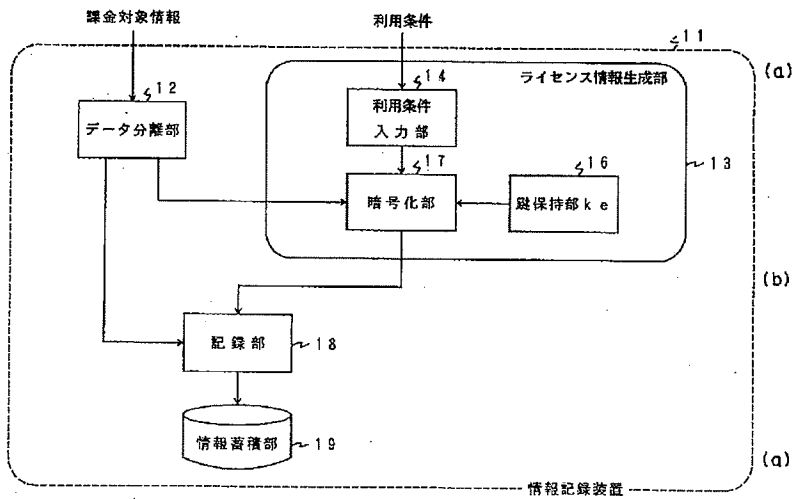
【補正内容】



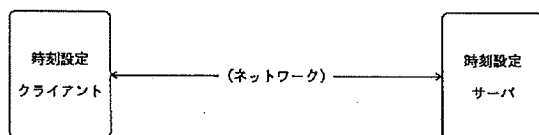
【図 1】



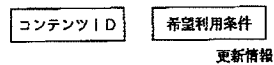
【図 3】



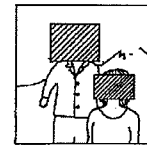
【図 17】



【図 116】



【図 5】



(b)

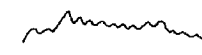


【図 6】

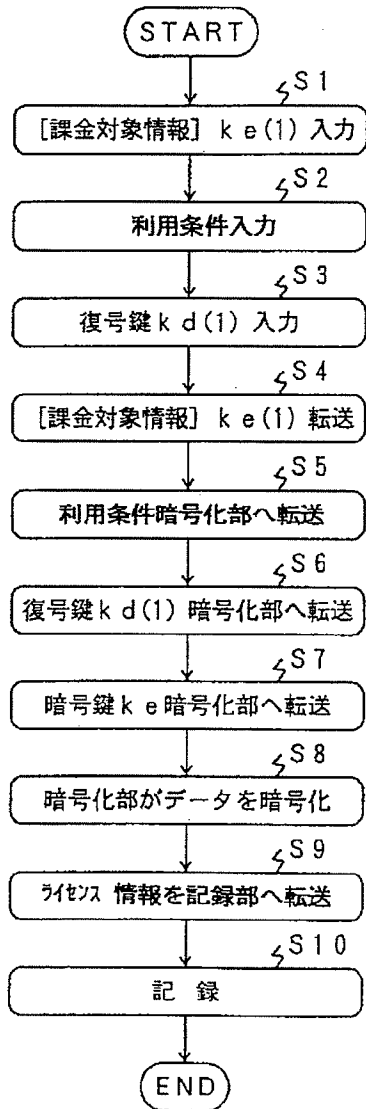
(a)



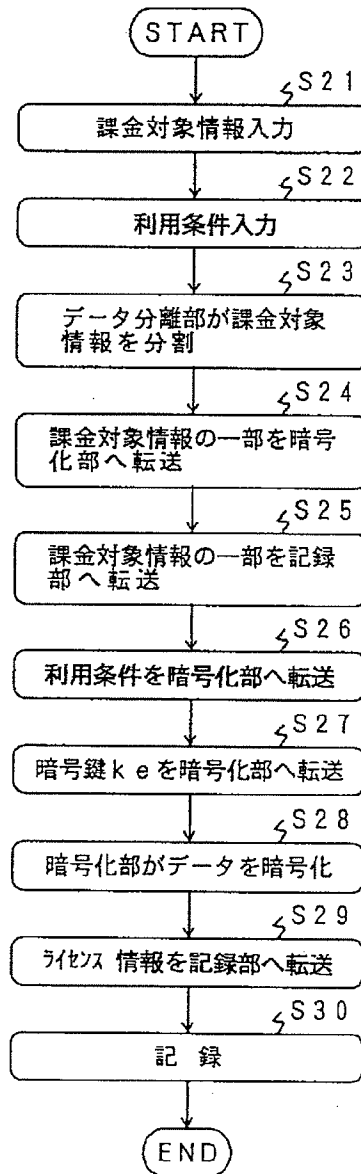
(b)



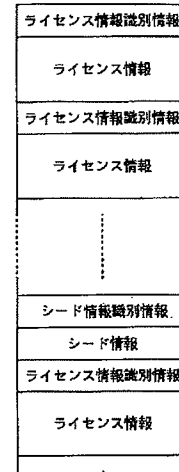
【図 2】



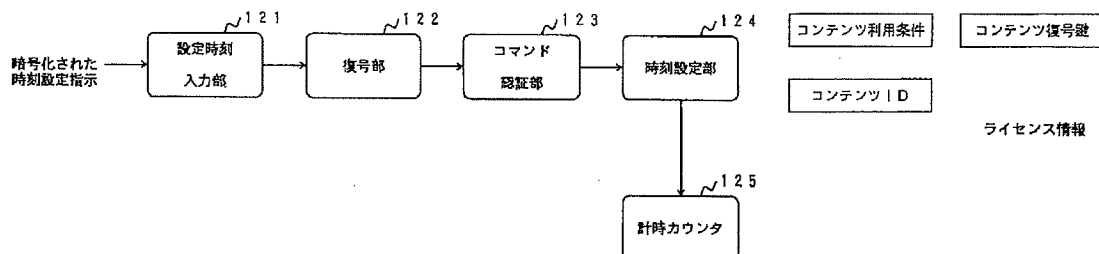
【図 4】



【図121】

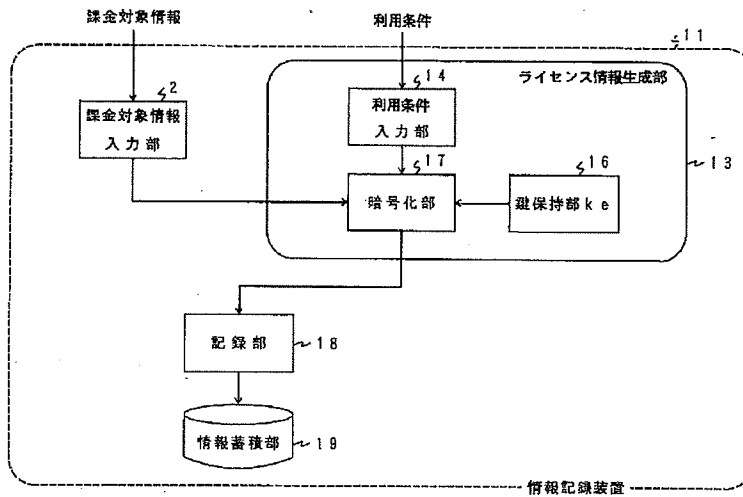


【図15】

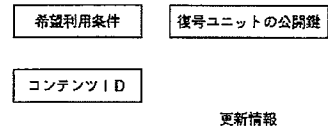


【図55】

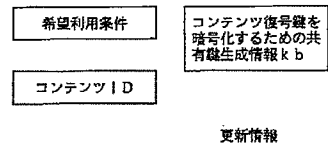
【図 7】



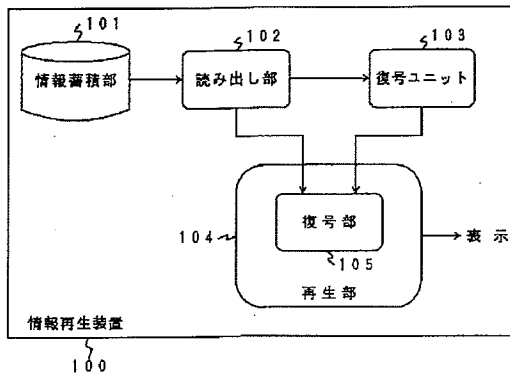
【図56】



【図62】



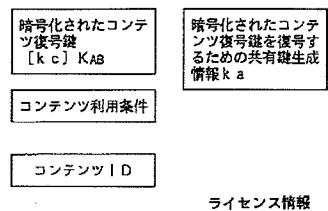
【図 8】



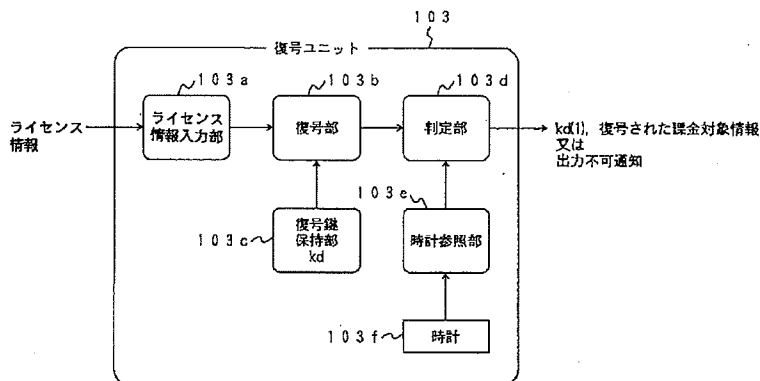
【図33】

課金対象情報ID	1週間	2週間	1ヵ月	支配先
ABCD	10円	15円	30円	abc

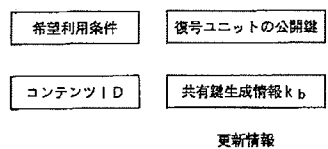
【図60】



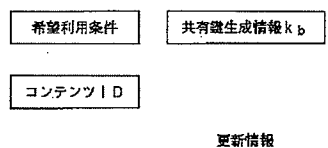
【図 9】



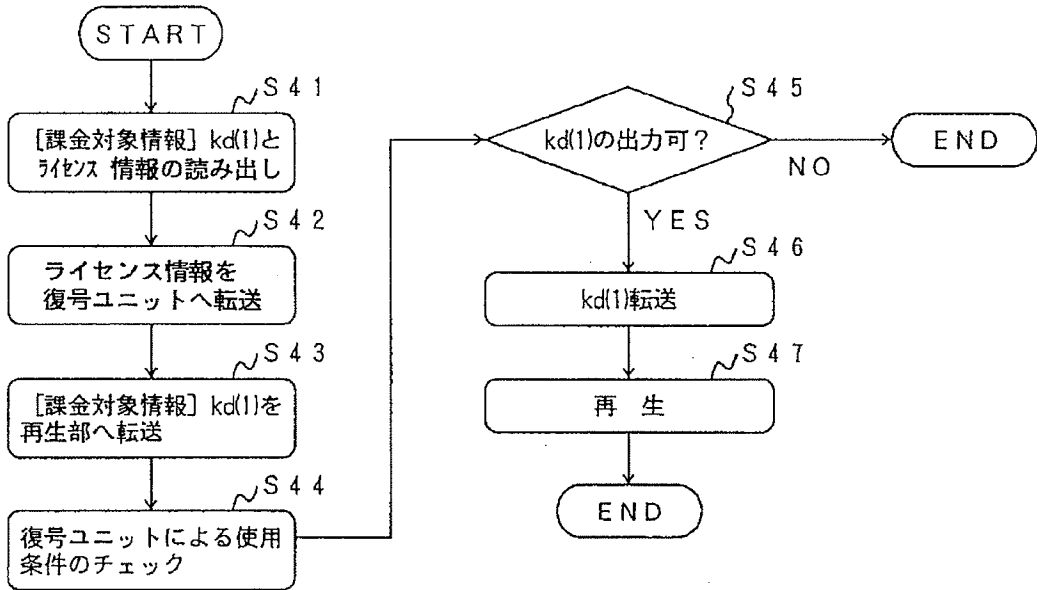
【図64】



【図69】

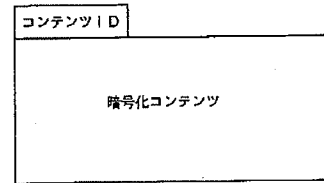
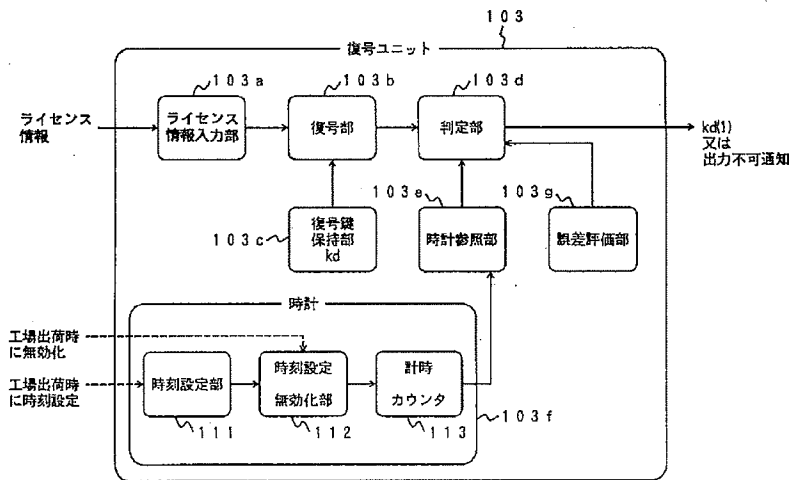


【図10】

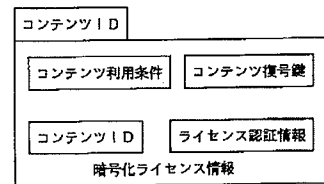


【図12】

【図113】

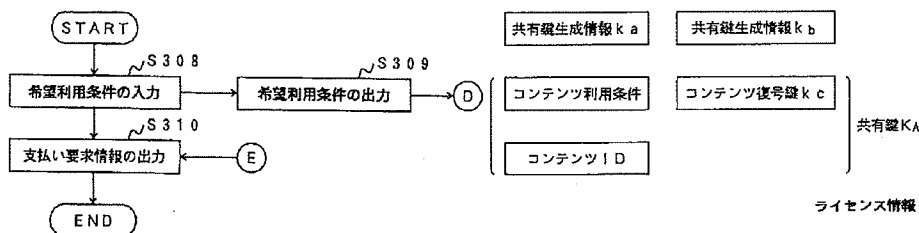


【図115】

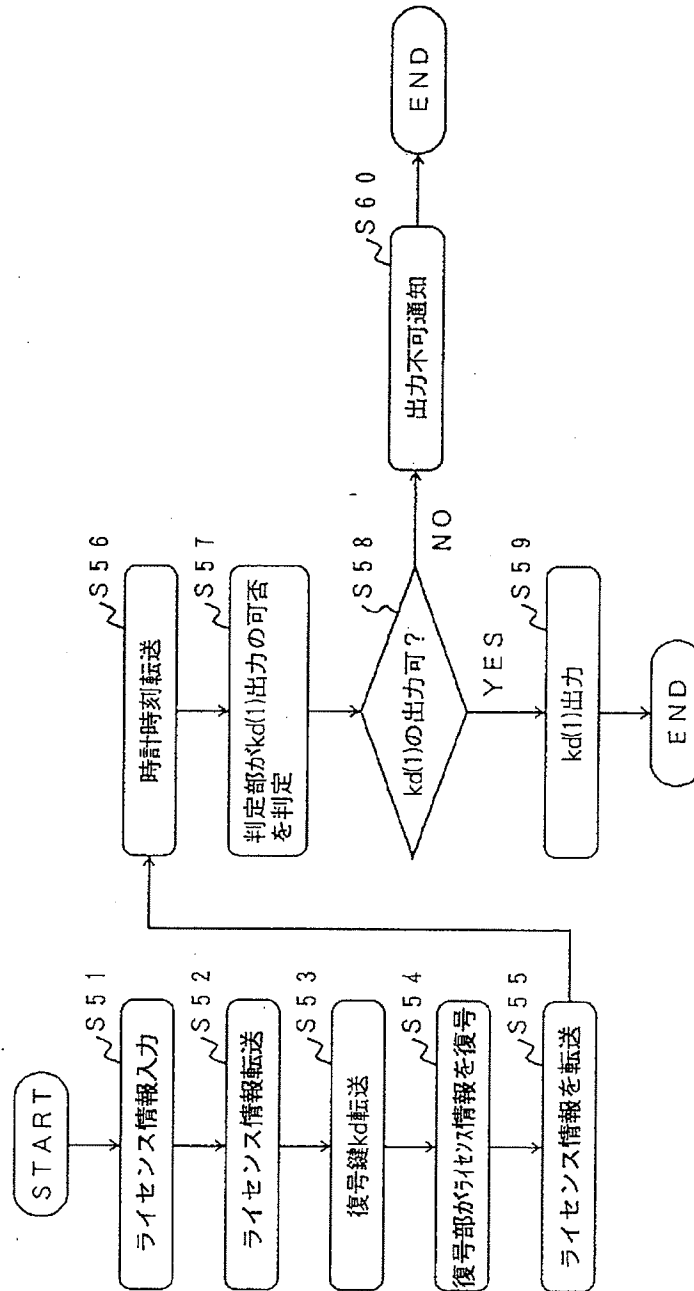


【図37】

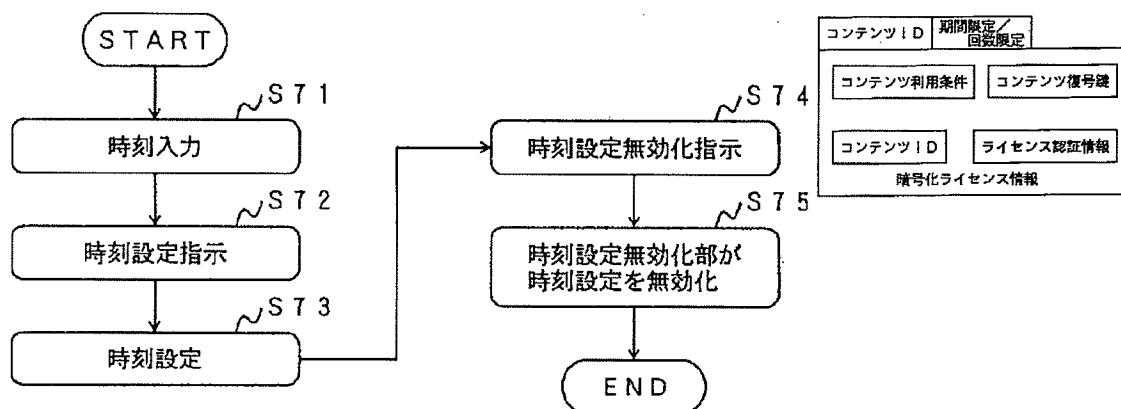
【図66】



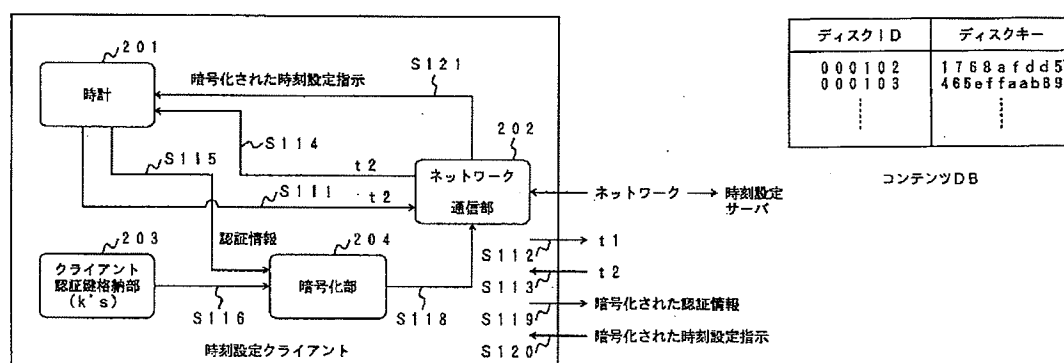
【図11】



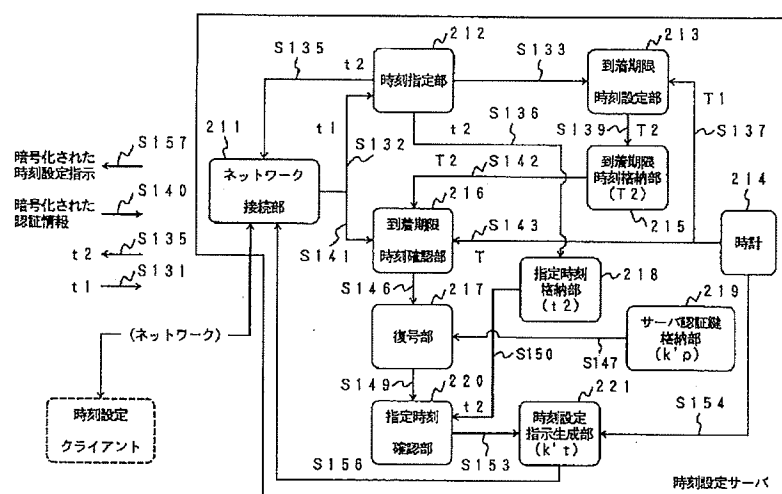
【図117】



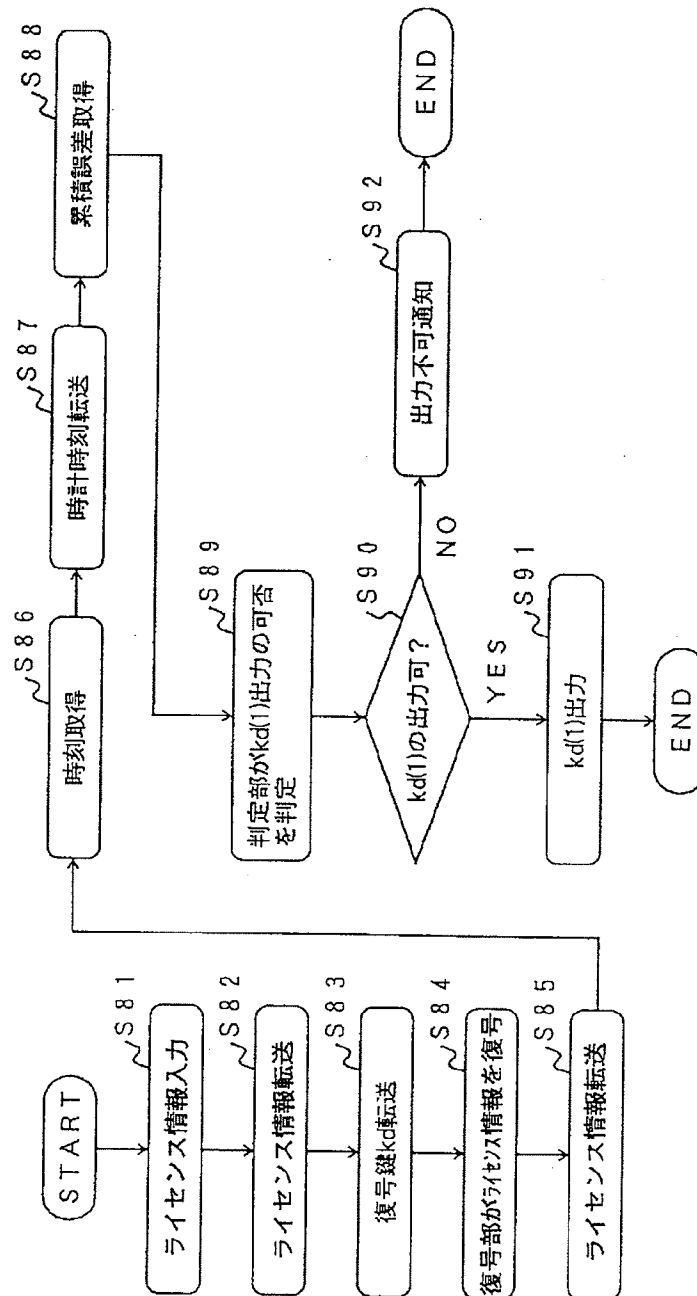
【図124】



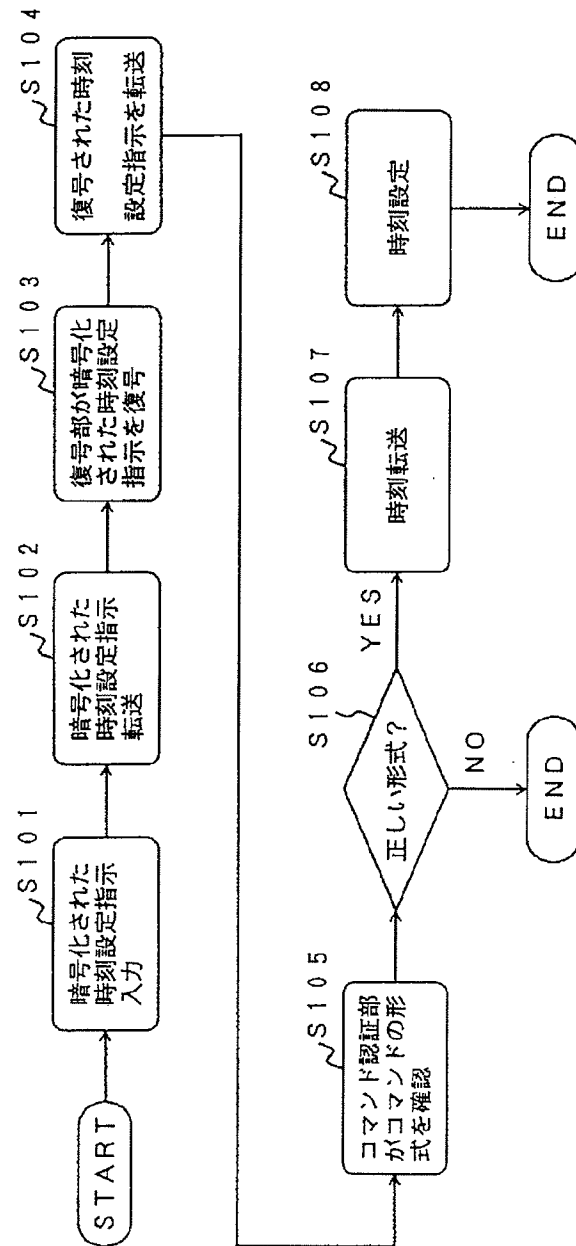
【图 19】



【図14】

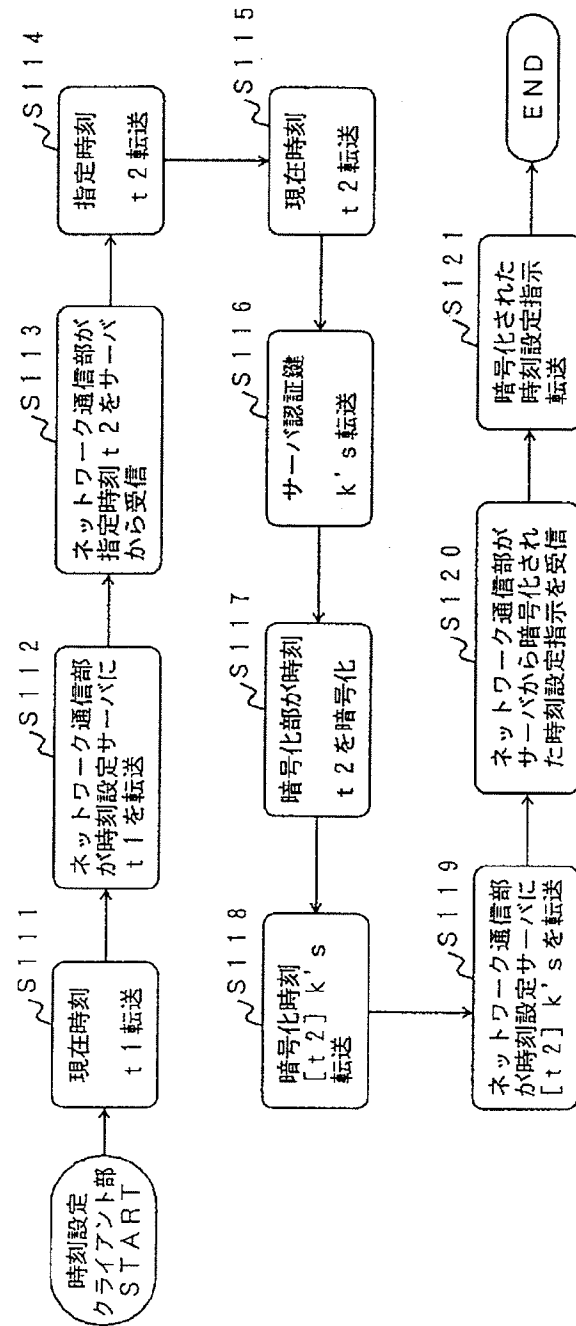


【図16】

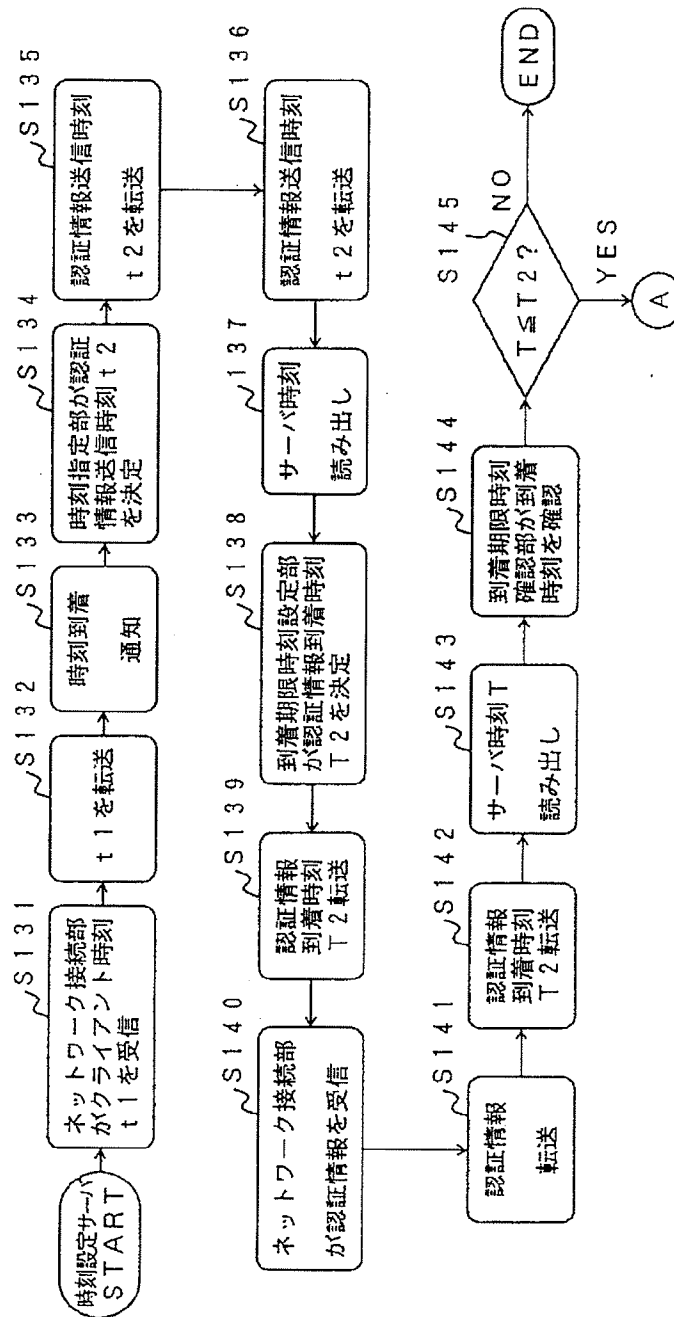




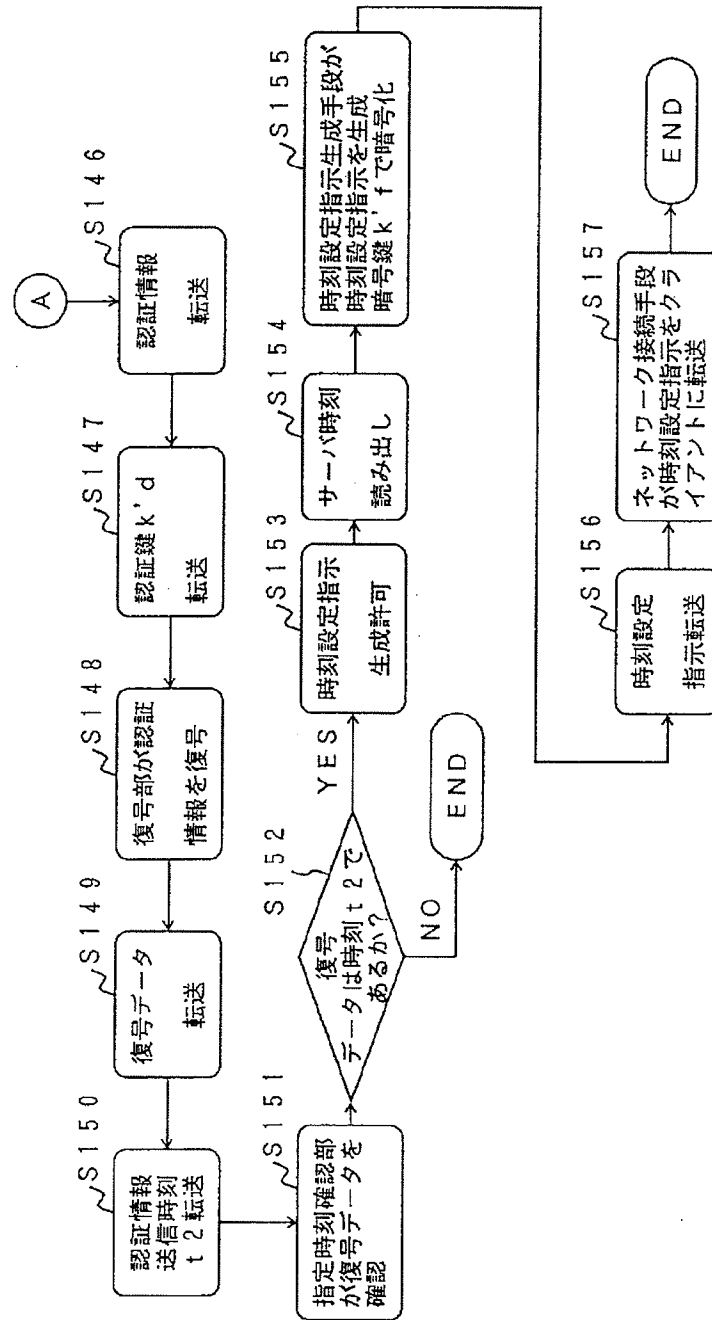
【図20】



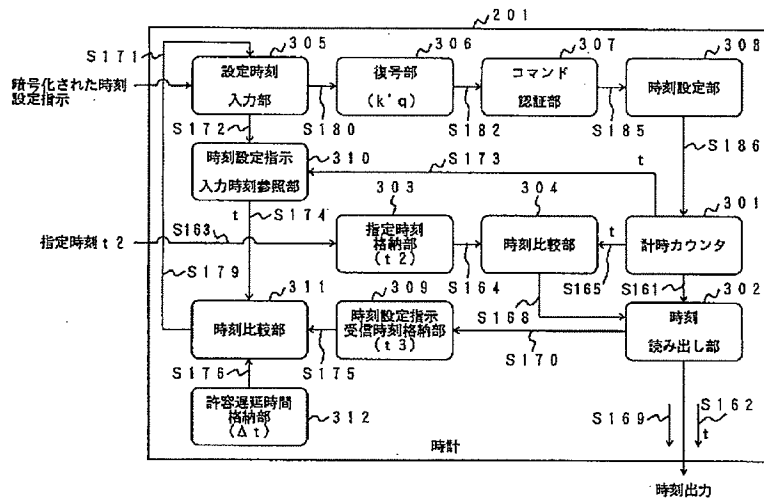
【図21】



【図22】



【図23】

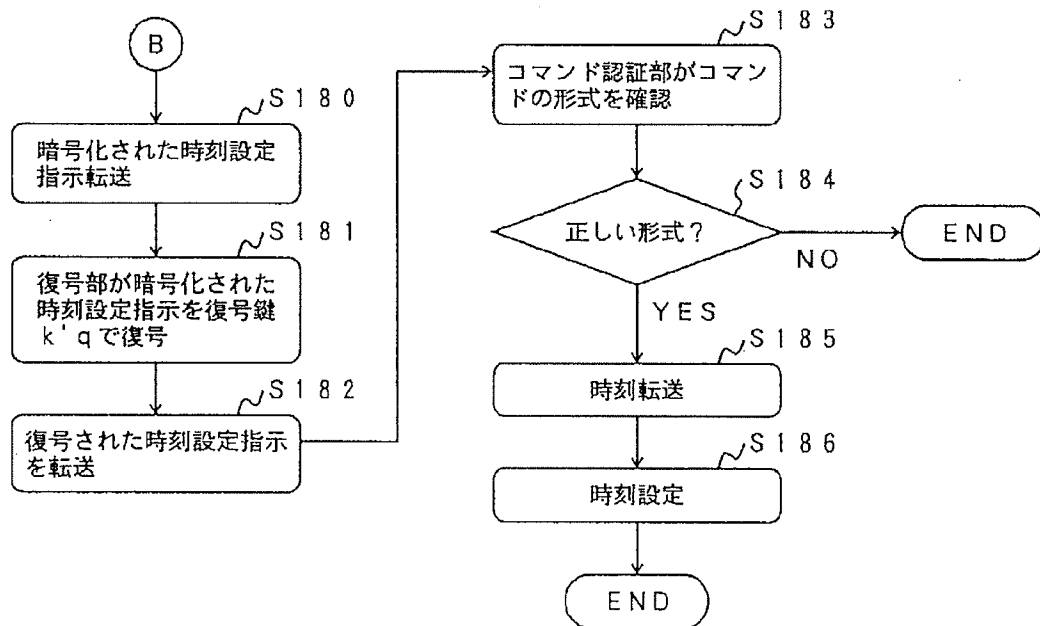


【図132】

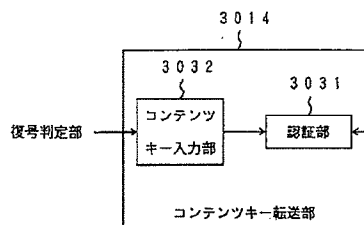
ディスクID	暗号化ディスク情報
0809eefd32	Fexx2039400x...
...	...

ライセンス注入装置 ライセンスDB

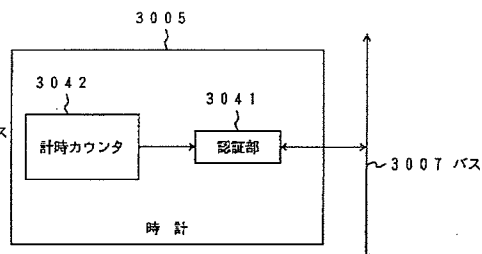
【図25】



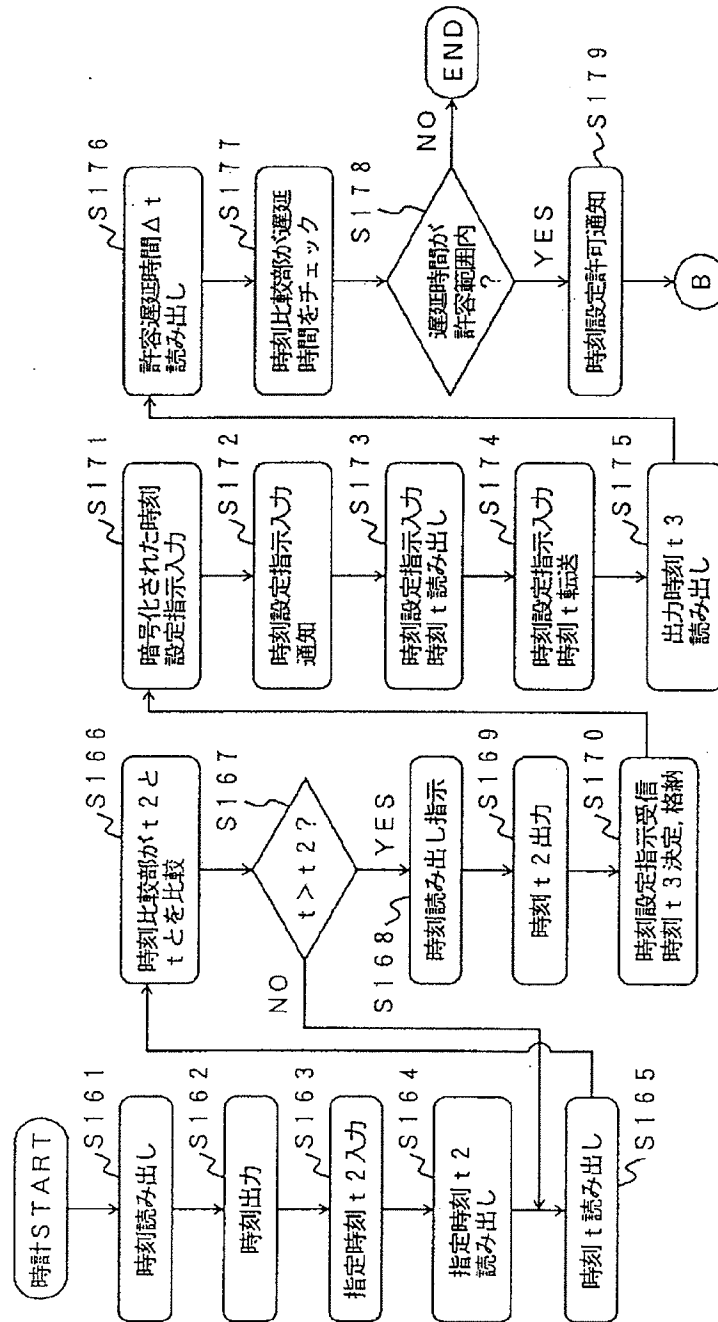
【図84】



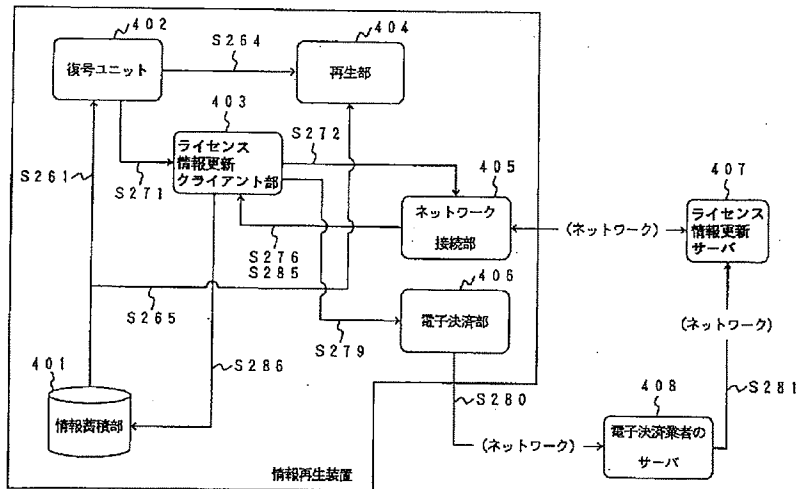
【図87】



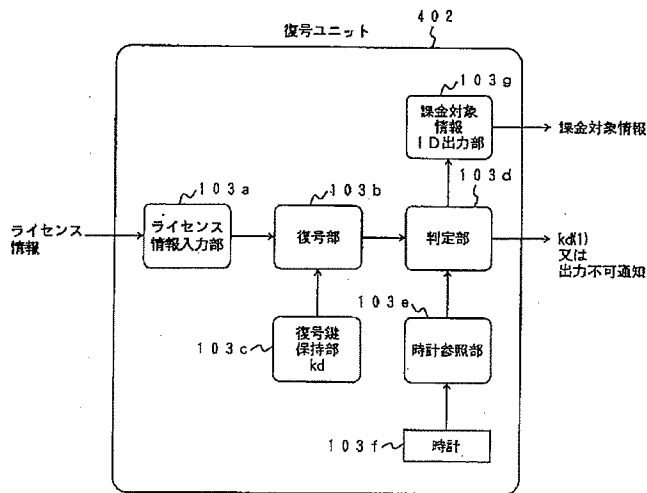
【図24】



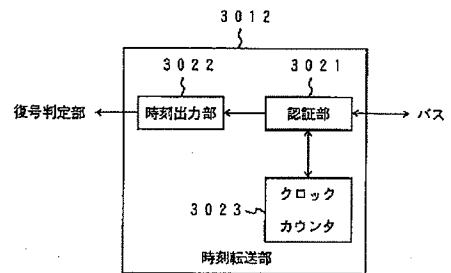
【図26】



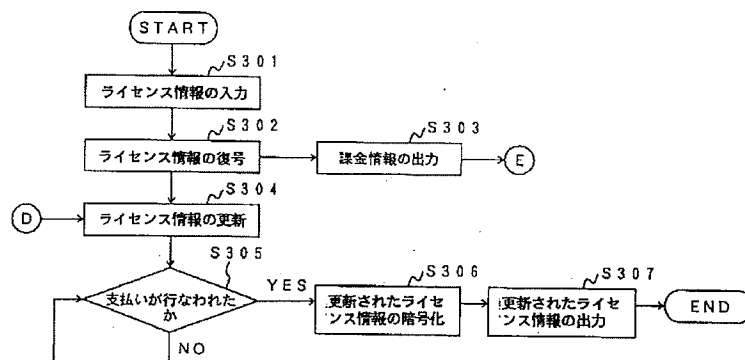
【図27】



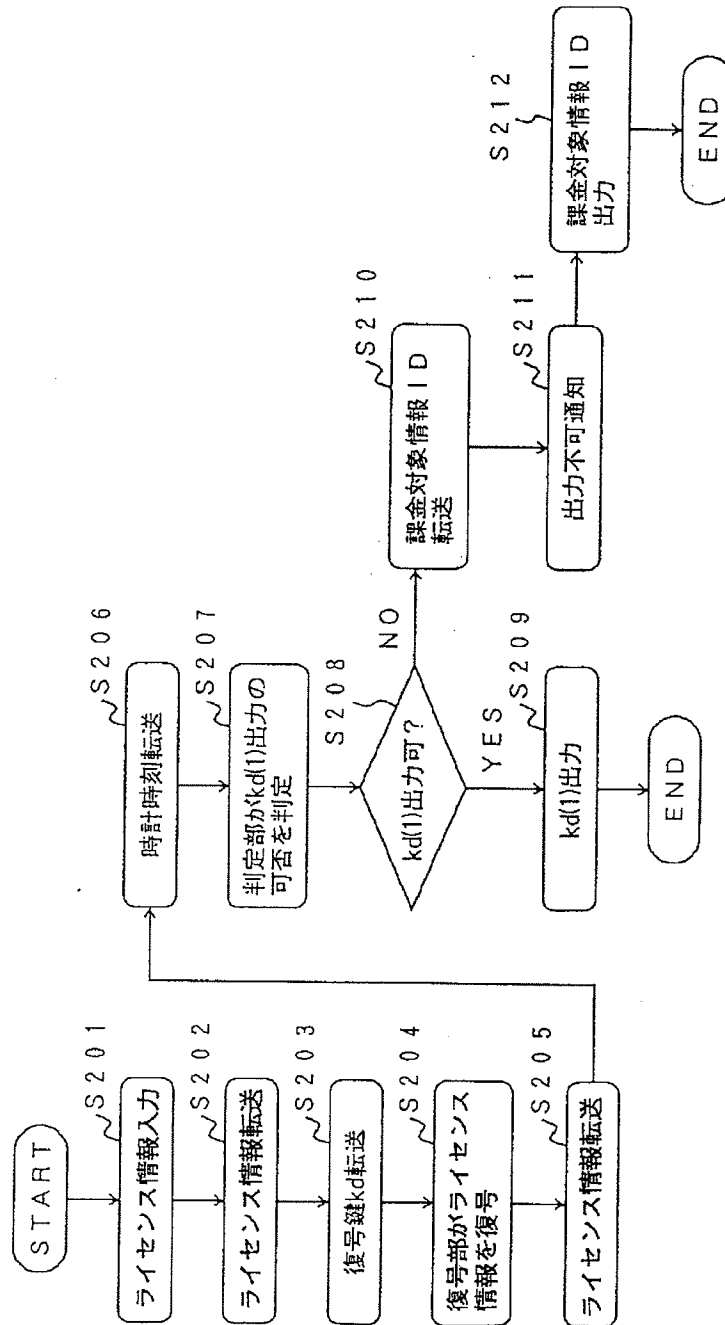
【図81】



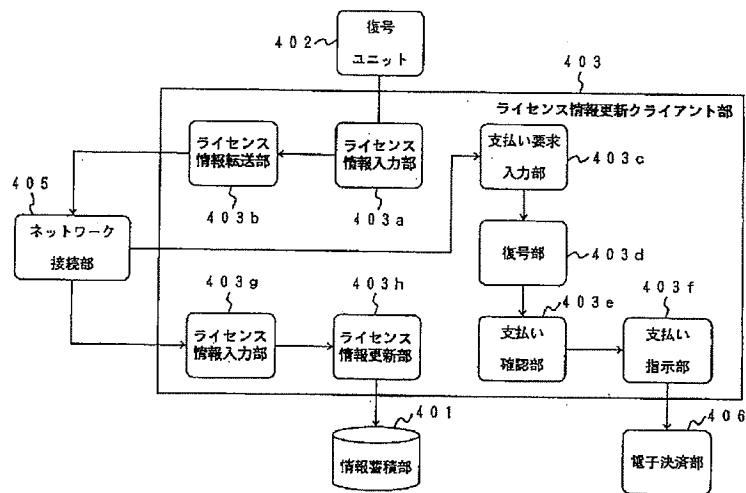
【図36】



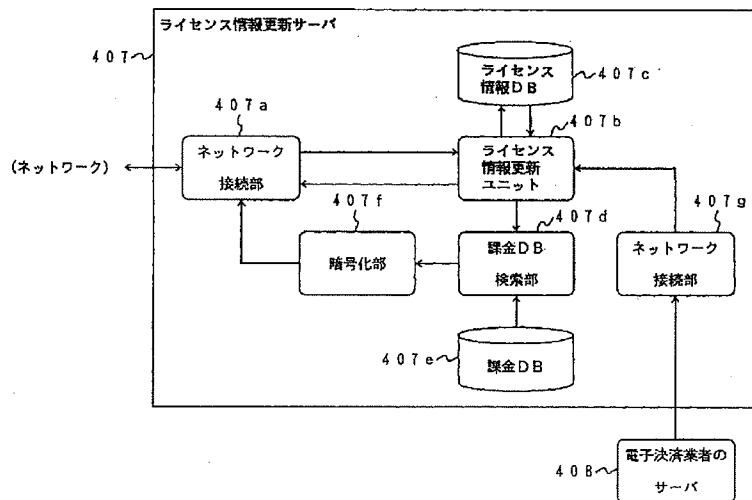
【図28】



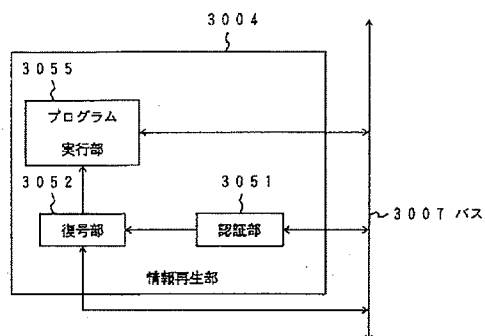
【図29】



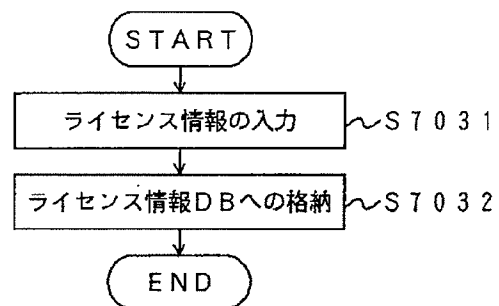
【図31】



【図96】

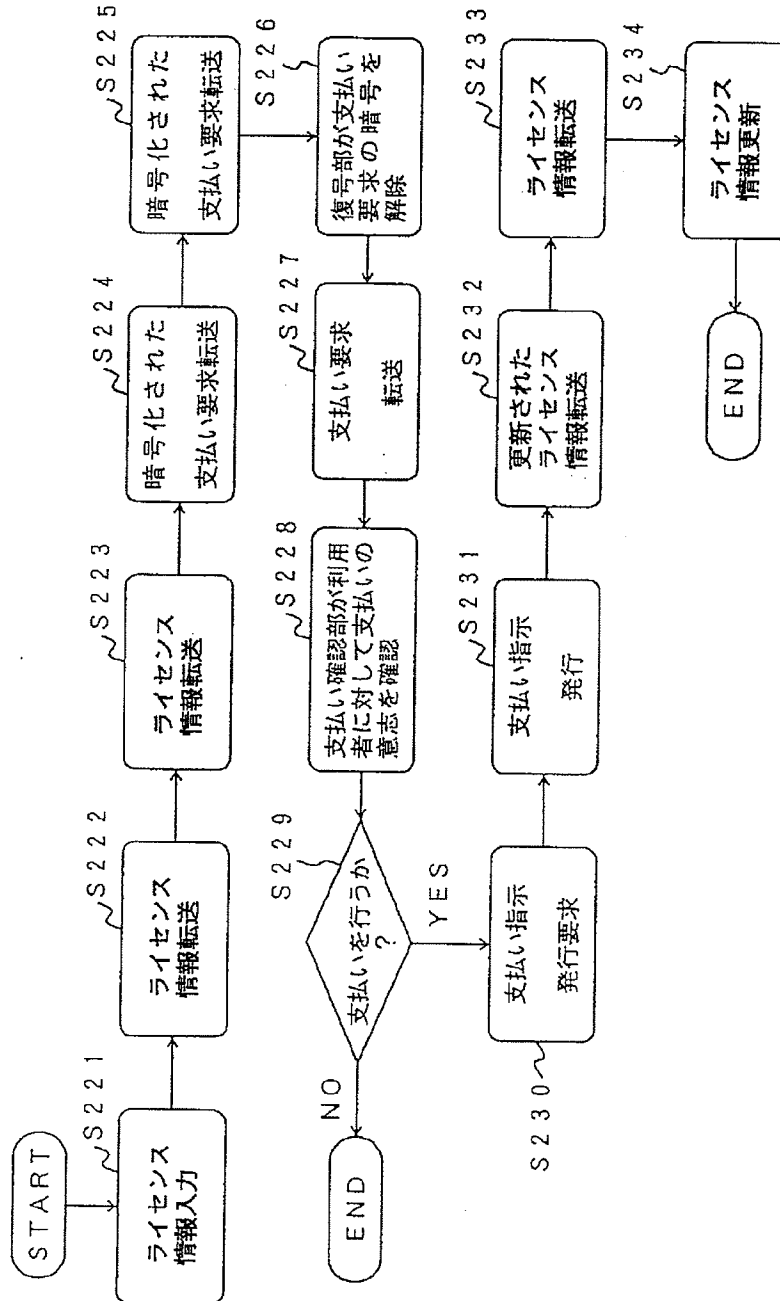


【図111】

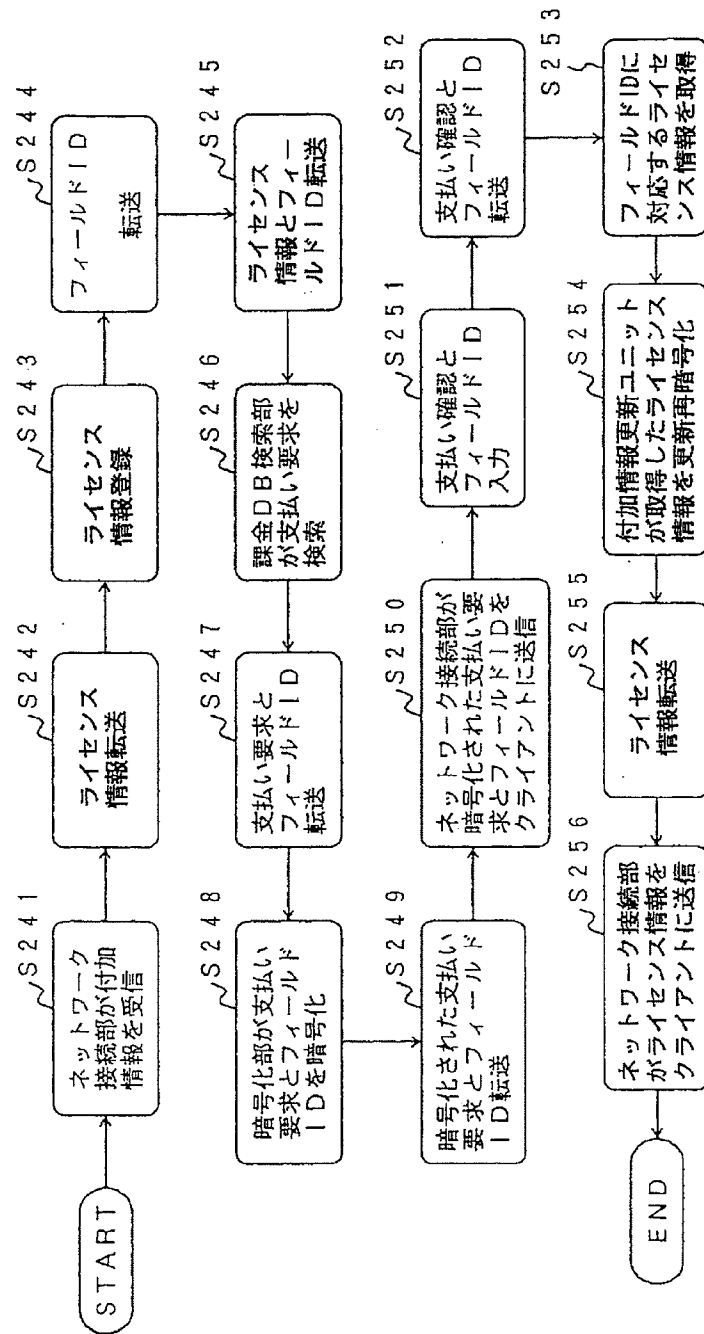




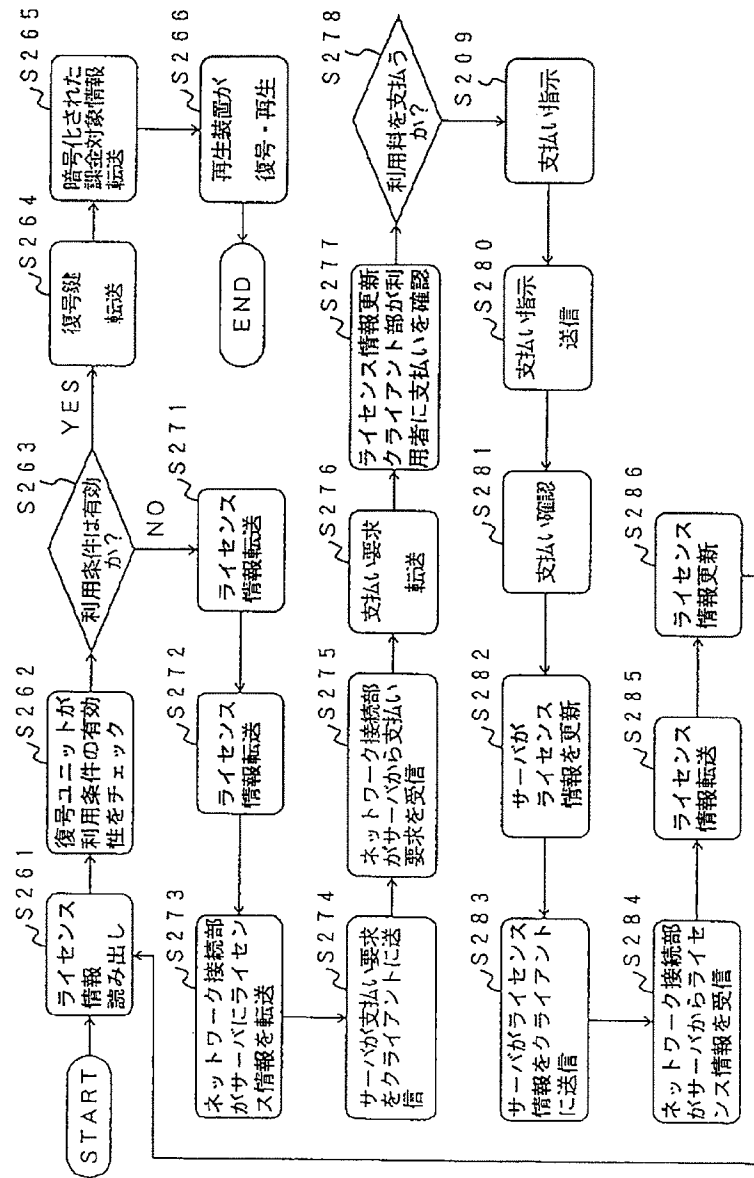
【図30】



【図32】



【図34】



```

graph TD
    In(( )) --> 501[ライセンス情報入力部 501]
    501 -- 502 --> 502[ライセンス情報更新部 502]
    502 <--> 503[復号鍵保持部 503]
    502 <--> 510[暗号鍵保持部 510]
    502 -- 505 --> 505[ライセンス情報番号部 505]
    502 -- 508 --> 508[支払い確認部 508]
    505 -- 508 --> 508
    505 -- 509 --> 509[更新ライセンス情報暗号化部 509]
    508 -- 509 --> 509
    509 -- 511 --> 511[更新ライセンス情報出力部 511]
    508 -- 507 --> 507[支払い要求出力部 507]
    507 --> Out(( ))
    508 -- 508 --> 508
    subgraph Unit [付加情報更新ユニット]
        501
        502
        503
        505
        507
        508
        509
        510
        511
    end

```

```

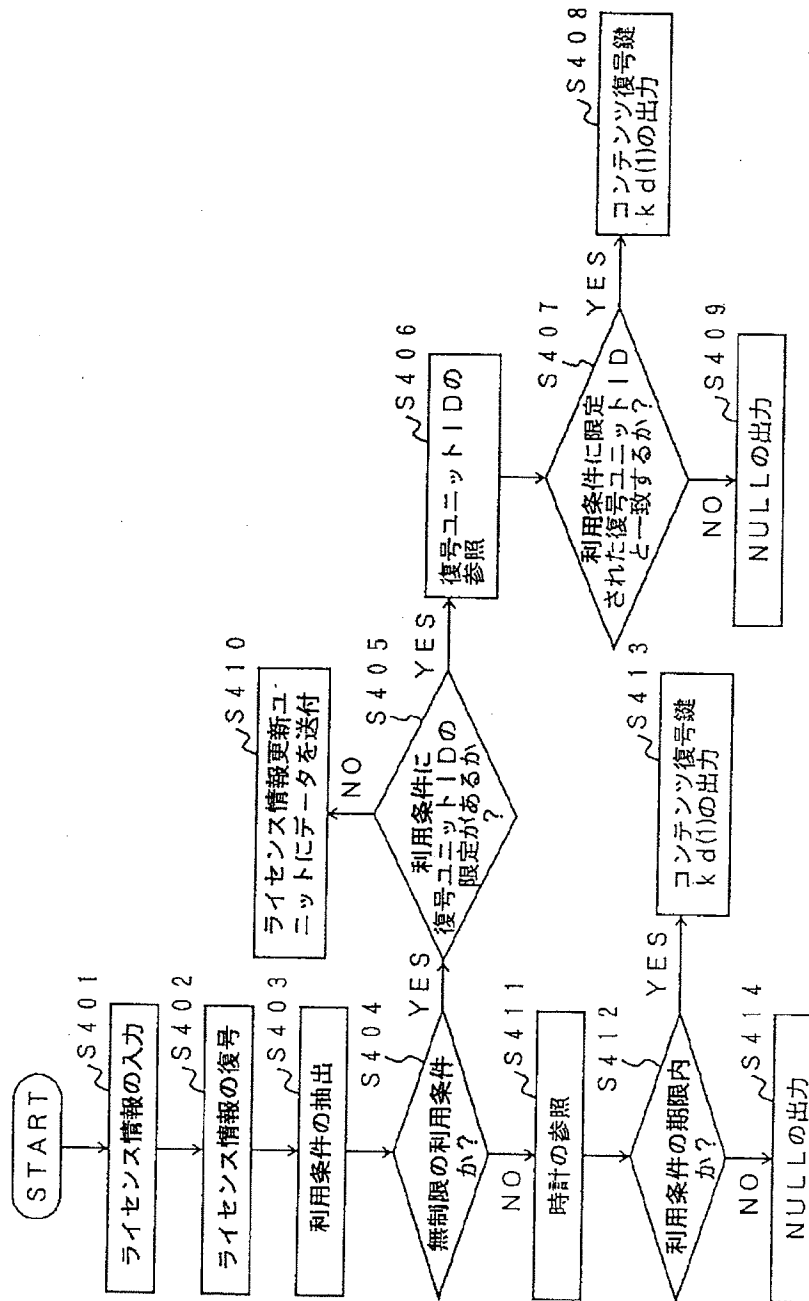
graph TD
    616[入力媒体  
(キーボード、マウス等)] --> 602[希望利用条件入力部]
    615[(記録媒体)] --> 601[レテックス情報読み込み部]
    602 --> 603[レテックス情報更新ユニット]
    601 --> 603
    603 <--> 607[更新レテックス情報書き込み部]
    603 --> 604[課金情報検索部]
    604 <--> 609[(課金情報DB)]
    603 --> 605[課金額情報出力部]
    605 --> 606[支払い判定部]
    606 --> 608[課金履歴管理部]
    608 <--> 610[(課金履歴DB)]
    607 --> 610
  
```

```

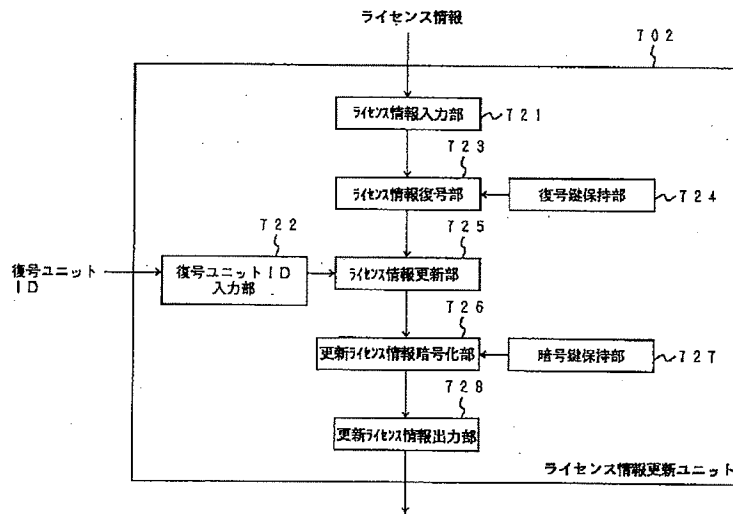
graph LR
    License[ライセンス情報] --> T11[ライセンス情報入力部 T11]
    T11 --> T12[復号部 T12]
    T12 --> T14[利用条件変更必要性判定部 T14]
    T14 -- YES --> T02[ライセンス情報更新ユニット T02]
    T14 -- NO --> T15[判定部 T15]
    T13[復号磁保持部 T13] --> T15
    T16[復号ユニットID参照部 T16] --> T15
    T15 -- "kd(1) or NULL" --> T12
    T15 --> T17[時計参照部 T17]
    T03[時計 T03] --> T17
    subgraph 701 [ ]
        T11
        T12
        T13
        T14
        T15
        T16
        T17
        T02
        T03
    end
    subgraph 703 [ ]
        T03
    end
    subgraph 702 [ ]
        T02
    end
    subgraph 704 [ ]
        T11
    end
    subgraph 705 [ ]
        T12
    end
    subgraph 706 [ ]
        T13
    end
    subgraph 707 [ ]
        T14
    end
    subgraph 708 [ ]
        T15
    end
    subgraph 709 [ ]
        T16
    end
    subgraph 710 [ ]
        T17
    end

```

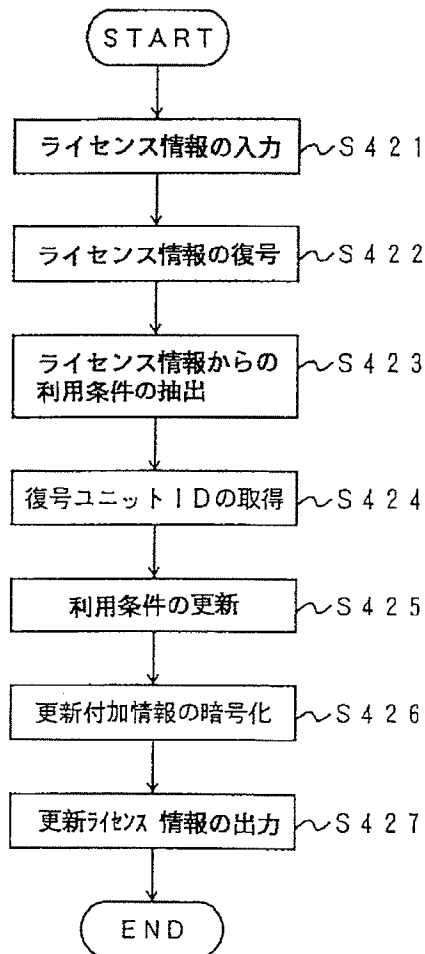
【図40】



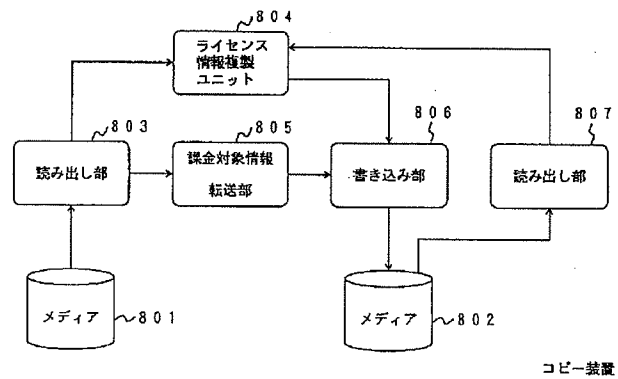
【図41】



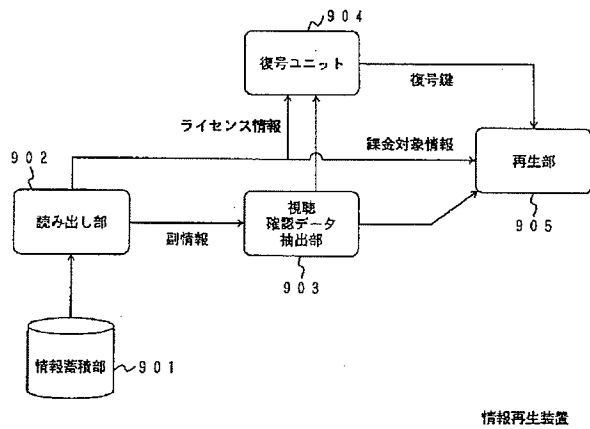
【図42】



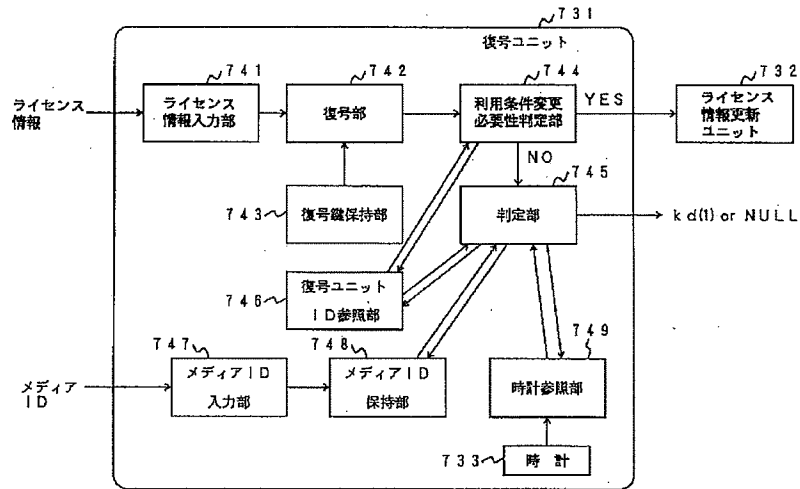
【図45】



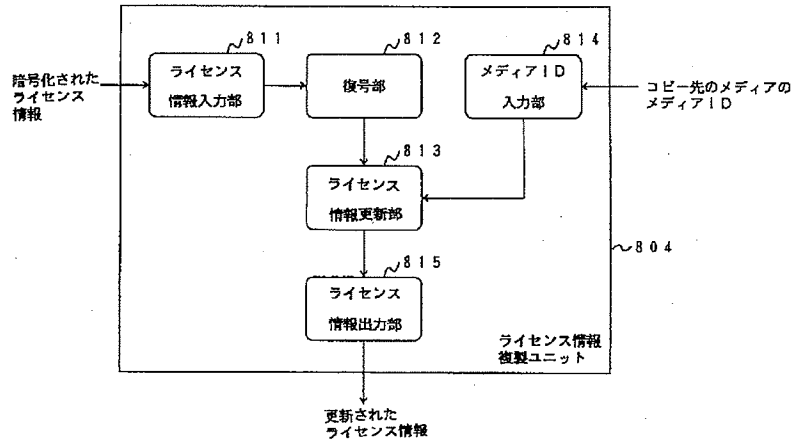
【図49】



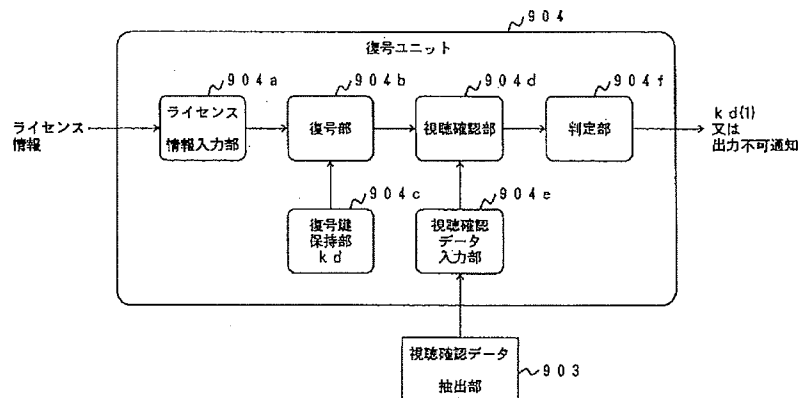
【図43】



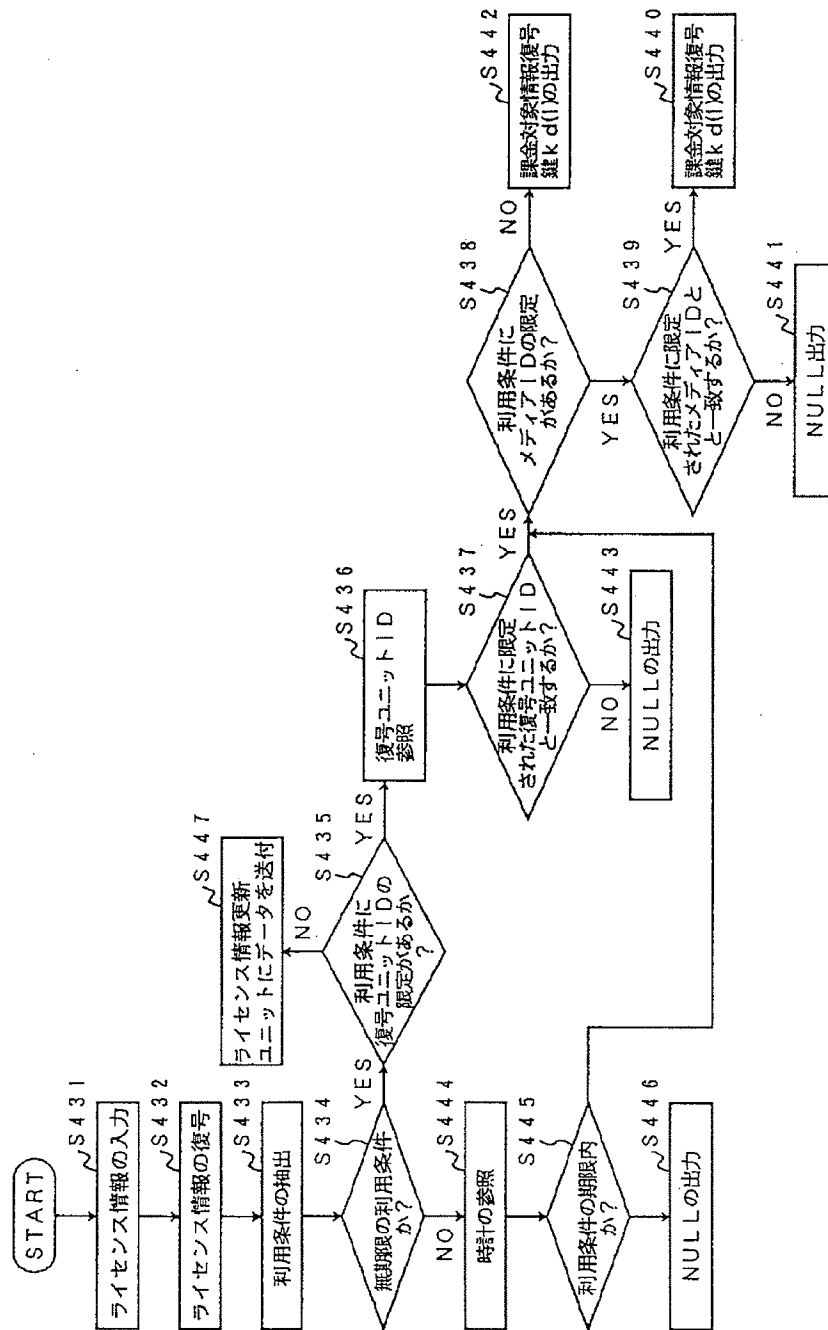
【図47】



【図51】

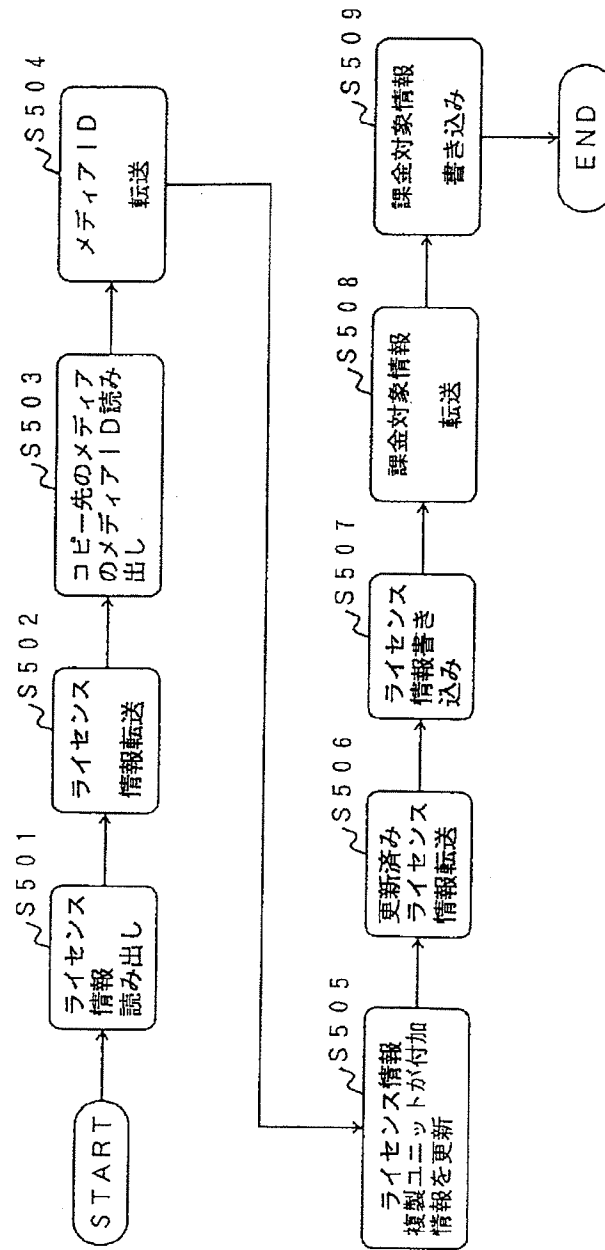


【図44】

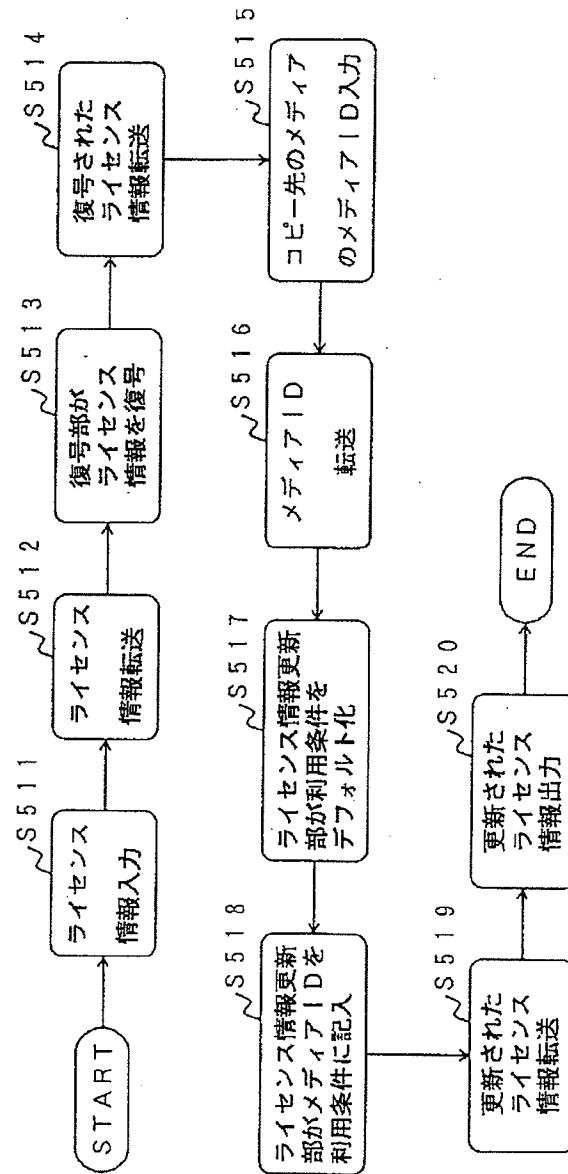




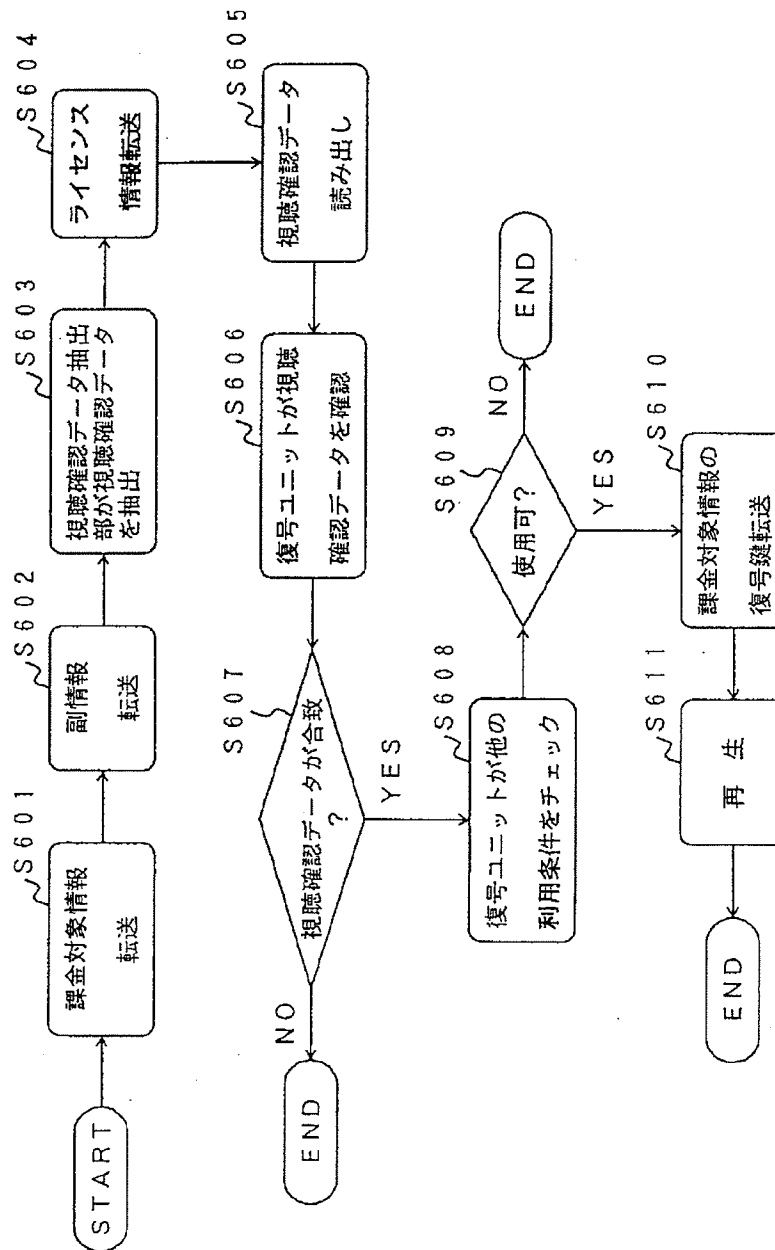
【図46】



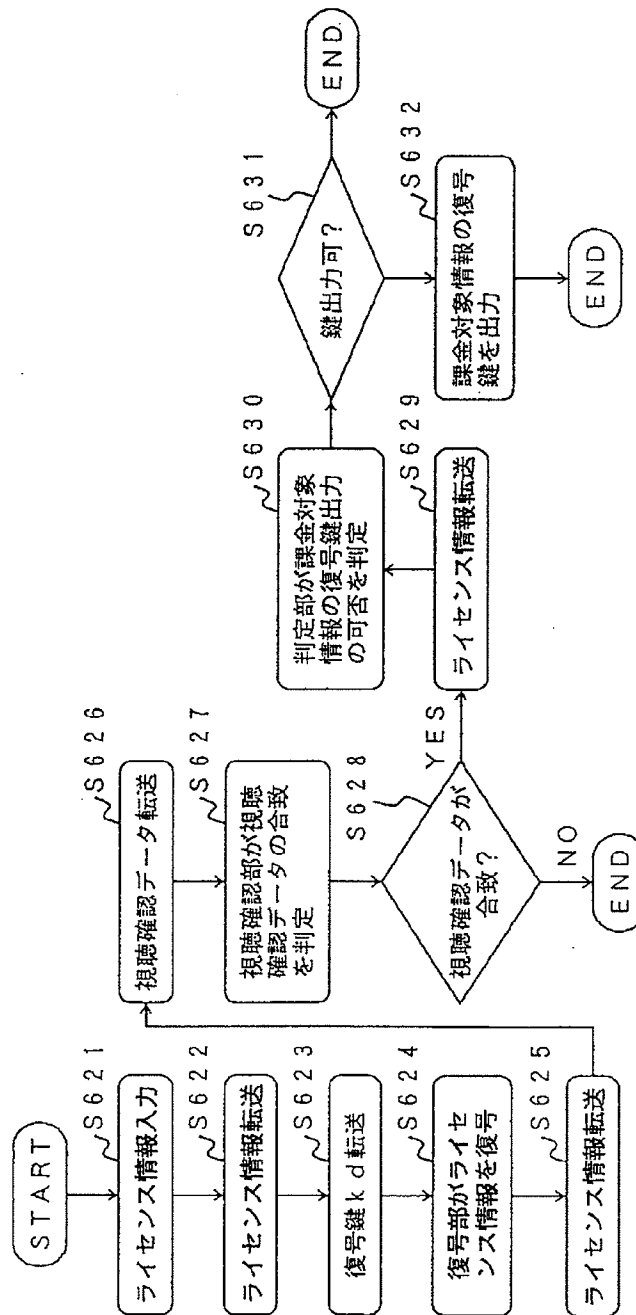
【図48】



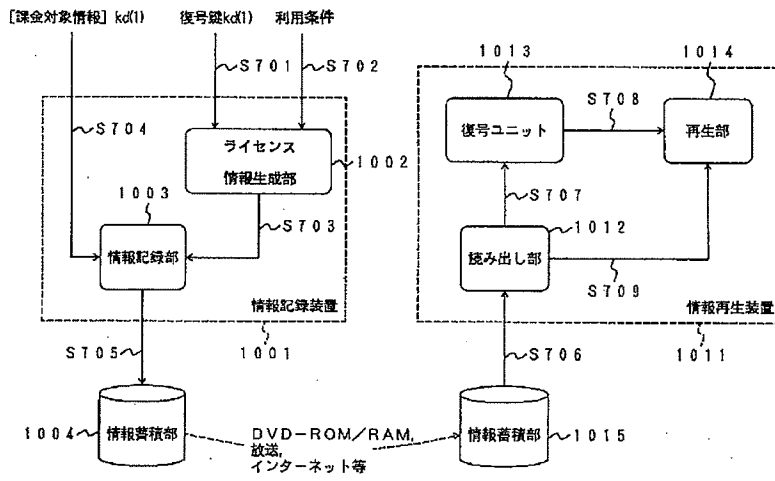
【図50】



【図52】

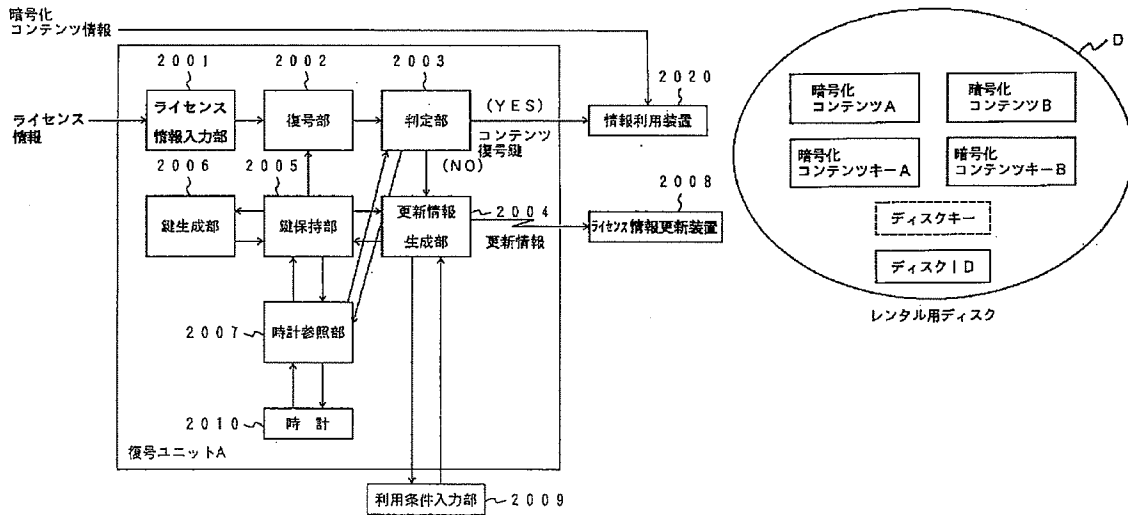


【図53】



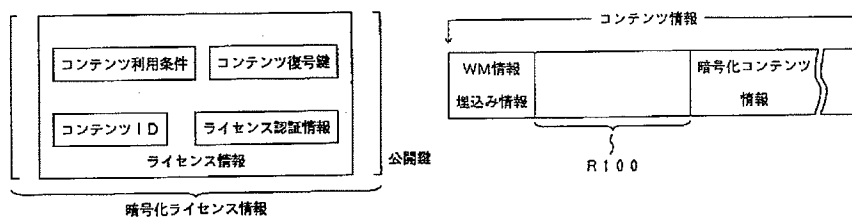
【図54】

【図123】

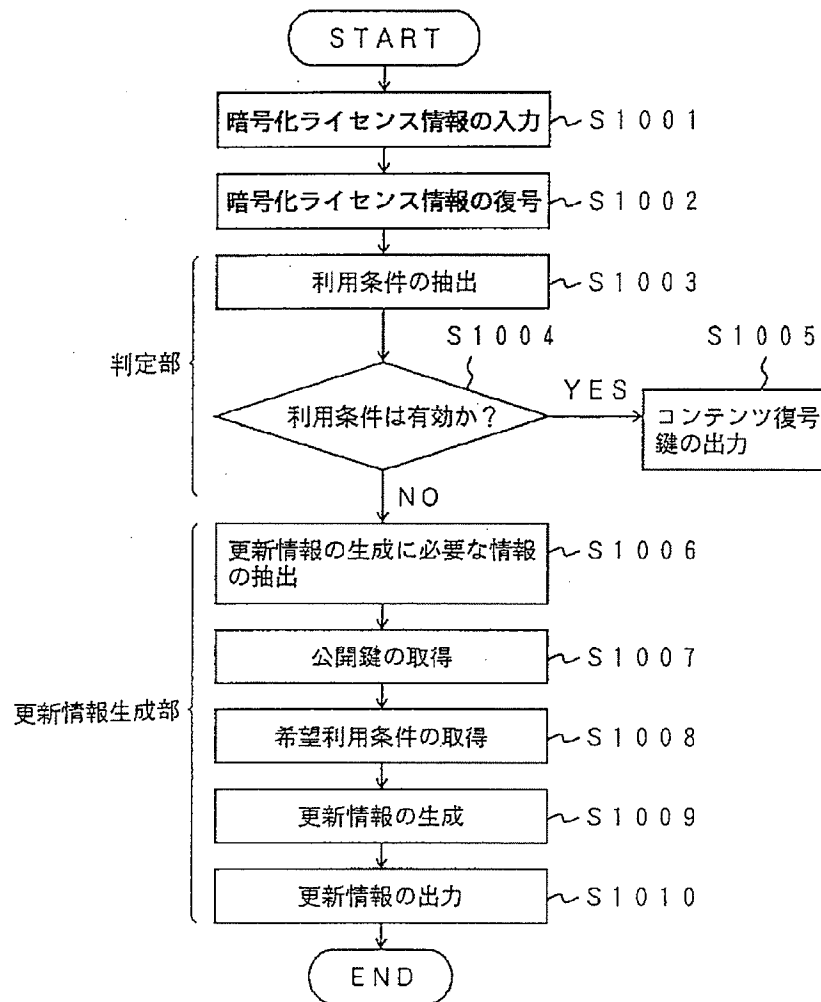


【図114】

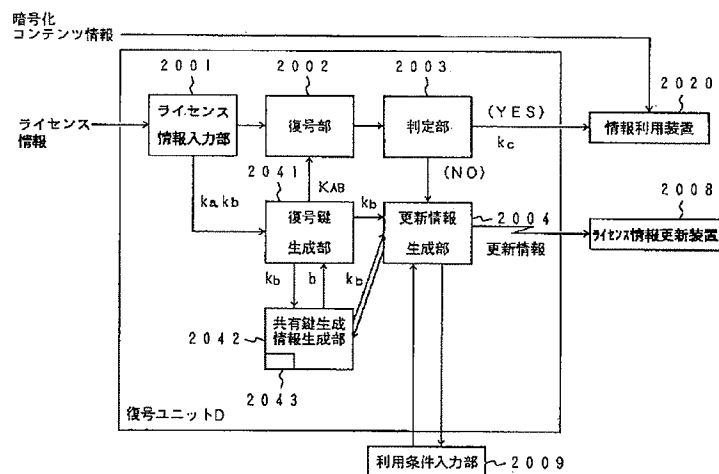
【図172】



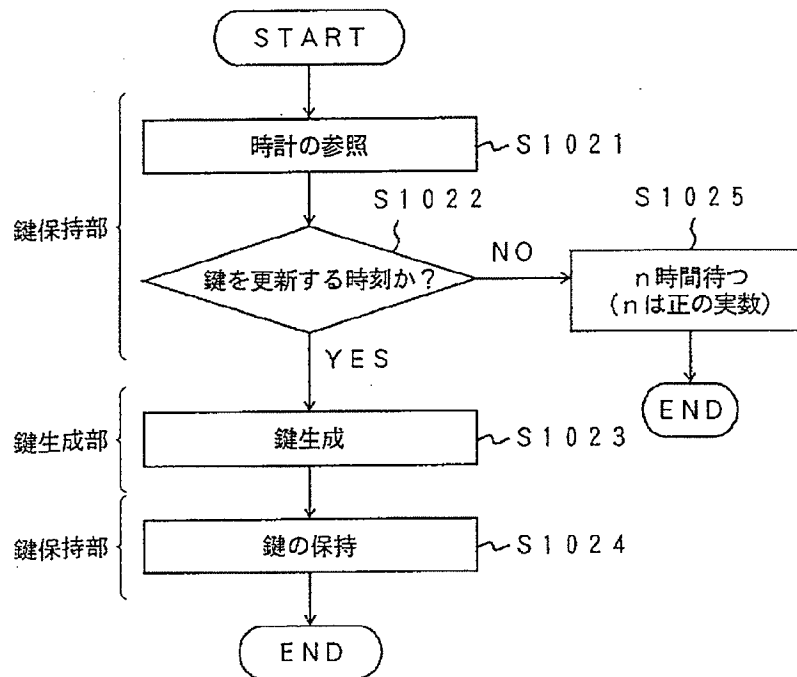
【図57】



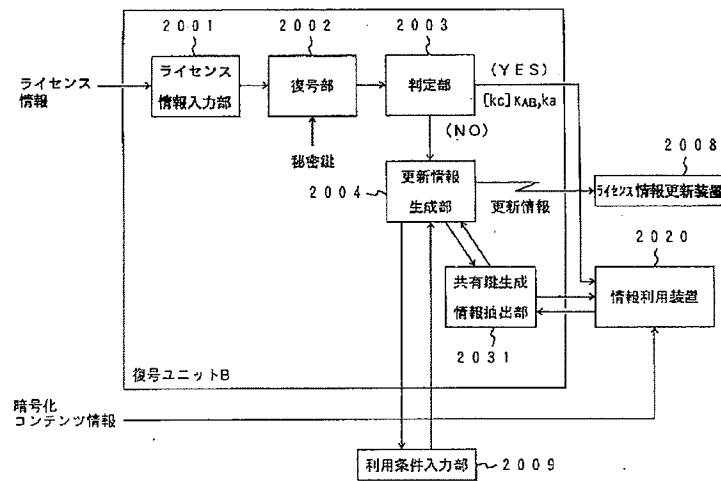
【図65】



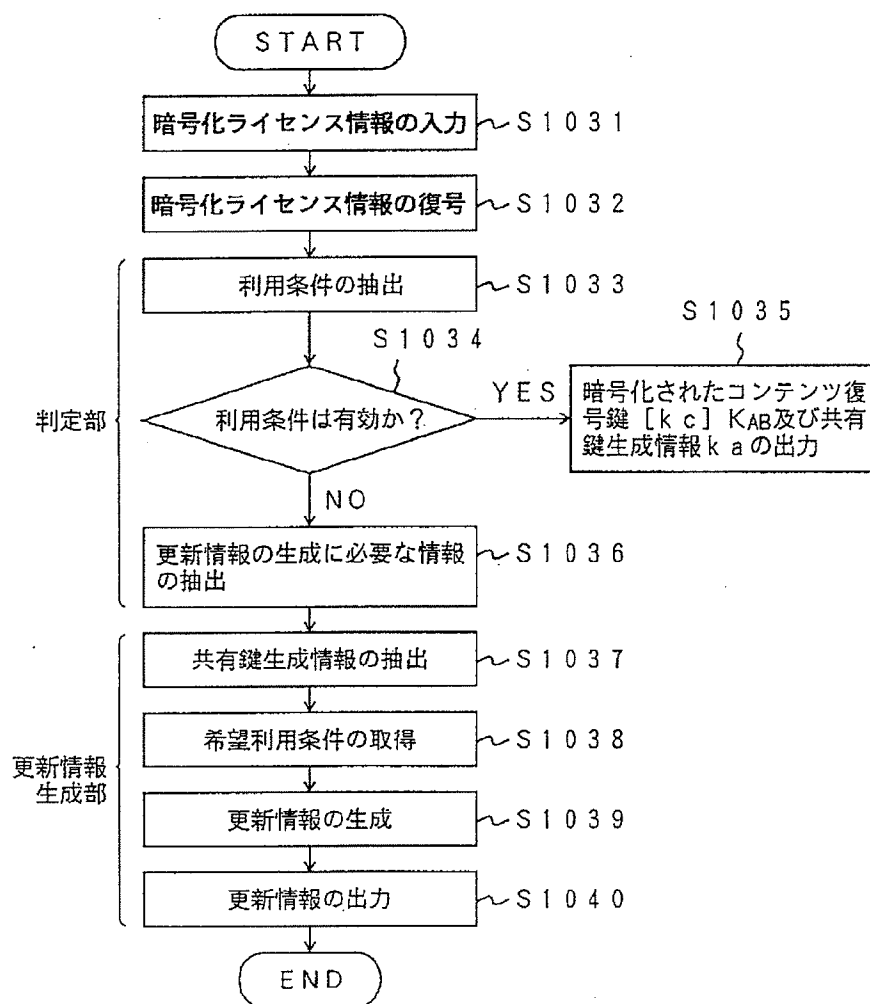
【図58】



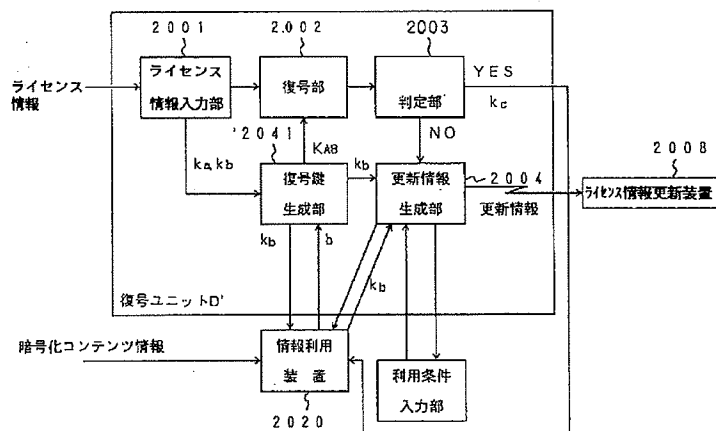
【図59】



【图 6 1】

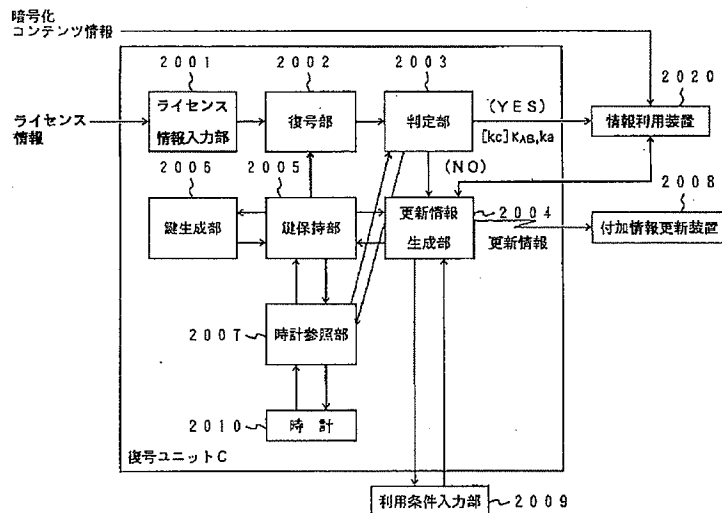


【図70】

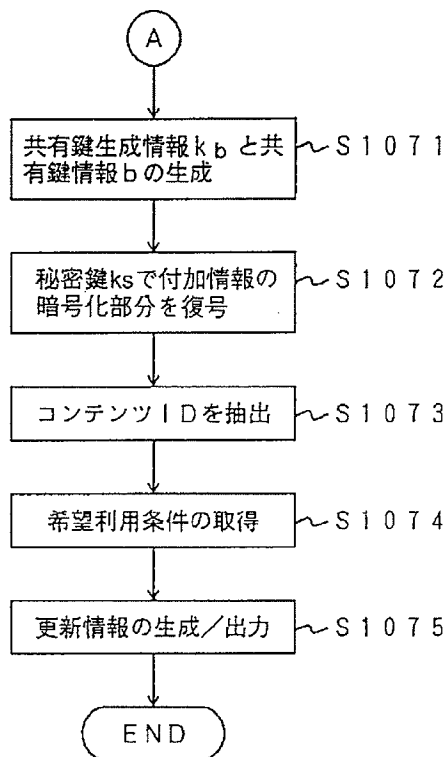




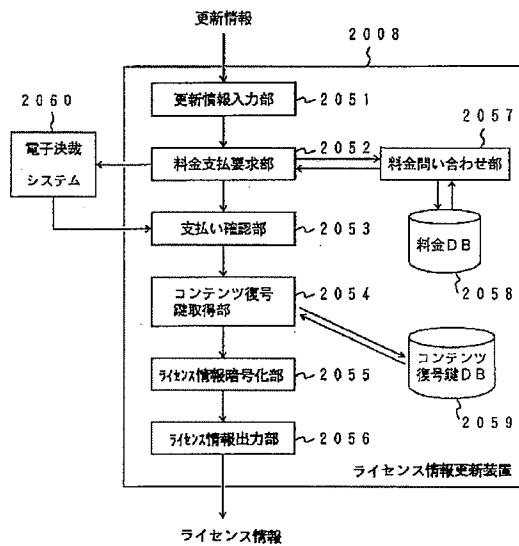
【図63】



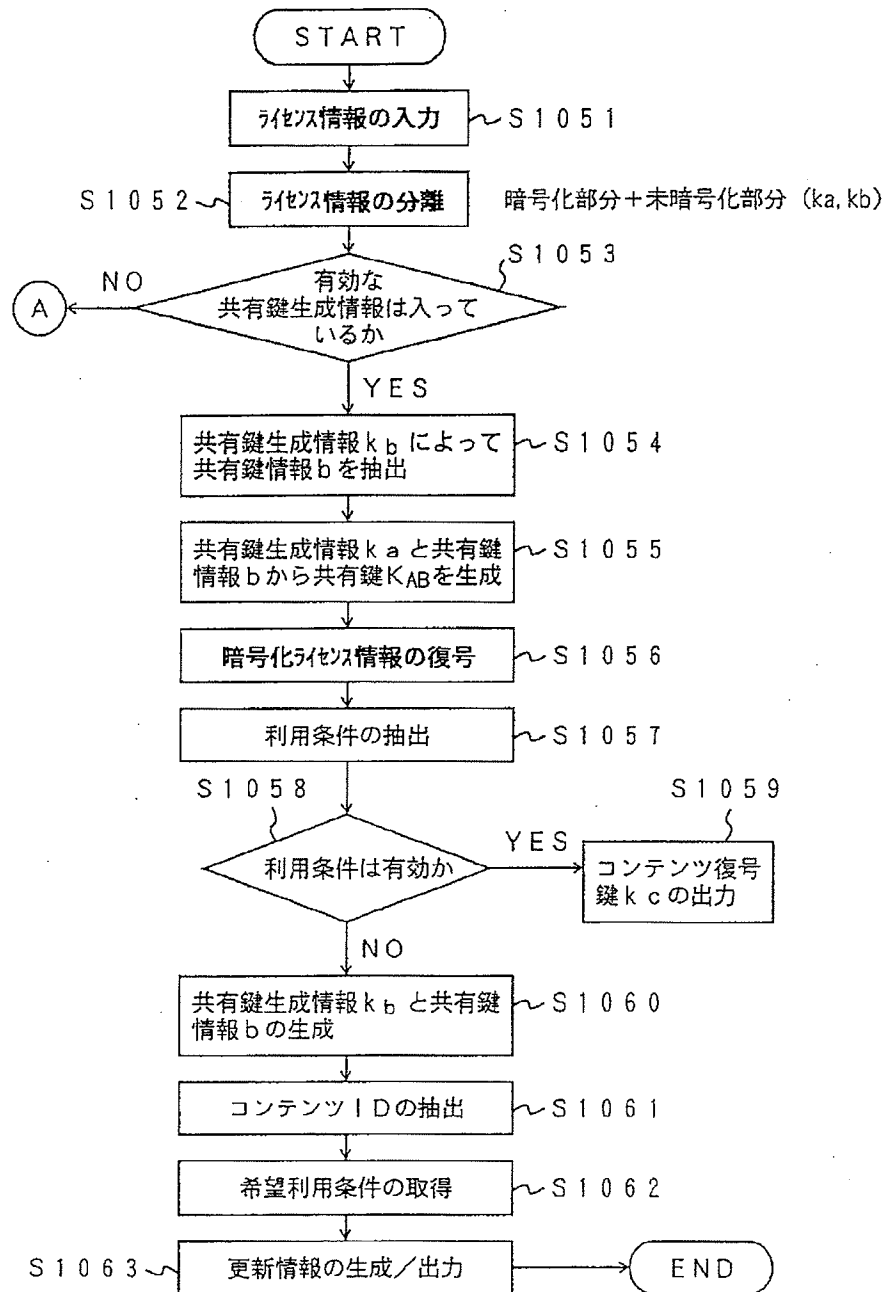
【図68】



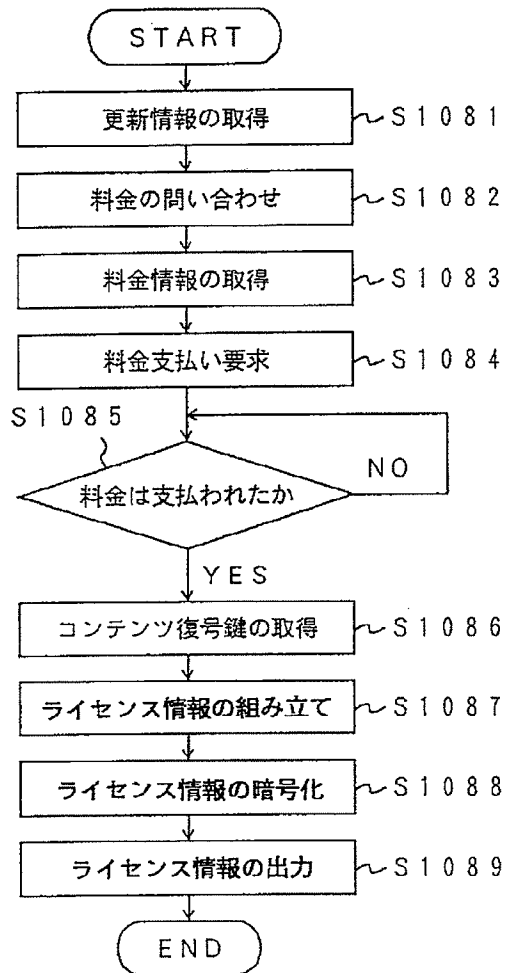
【図71】



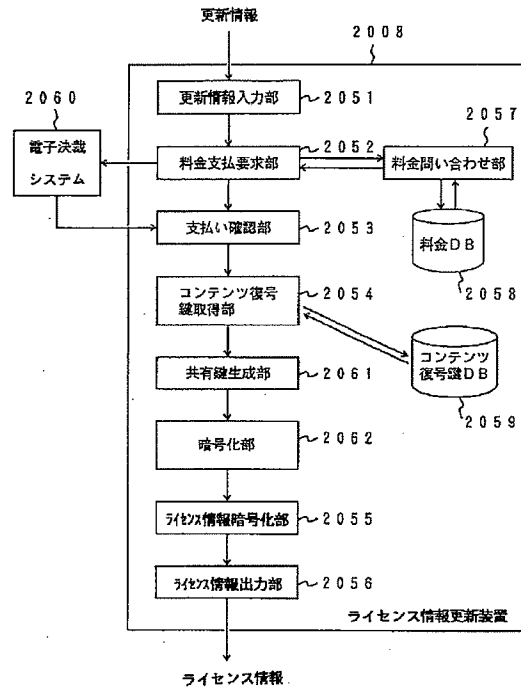
【図67】



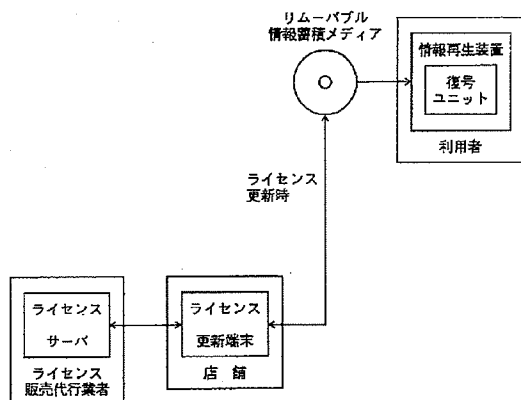
【図72】



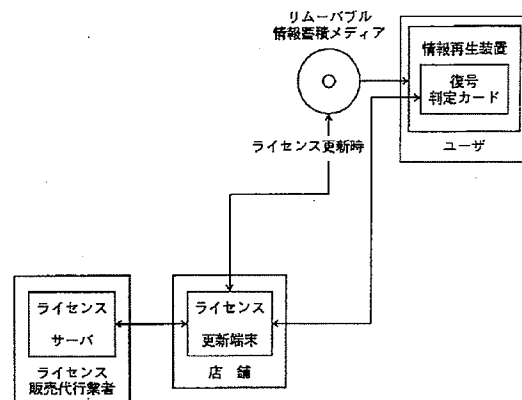
【図73】



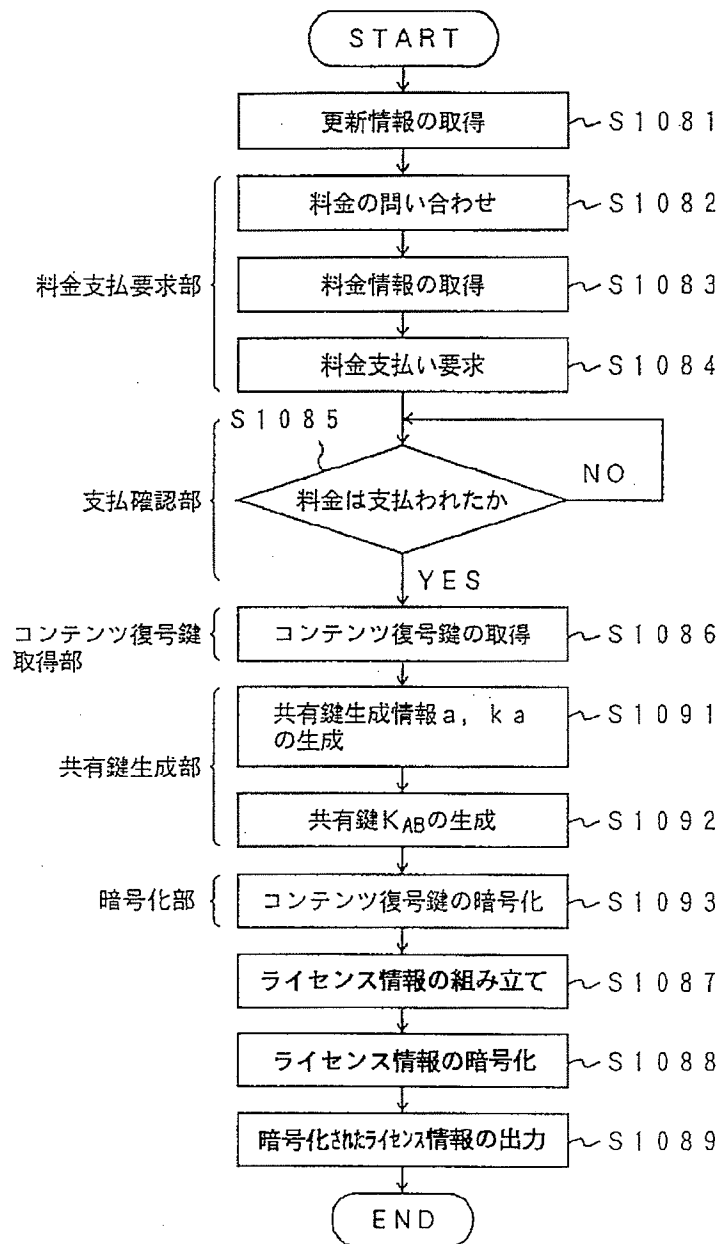
【図75】



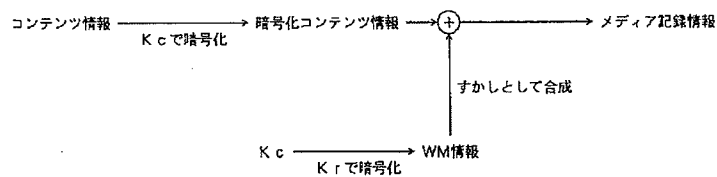
【図76】



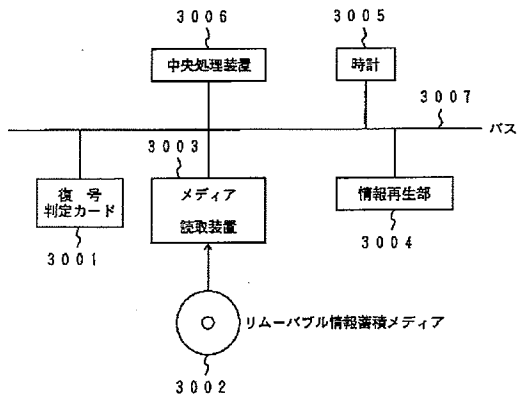
【図74】



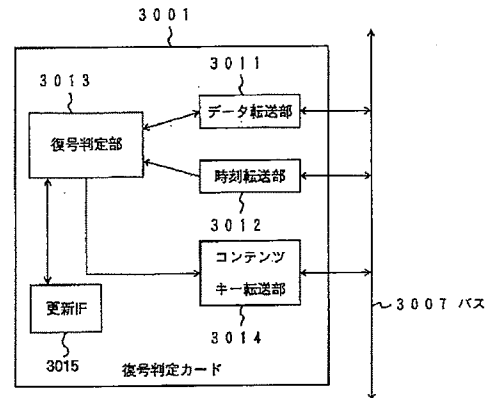
【図166】



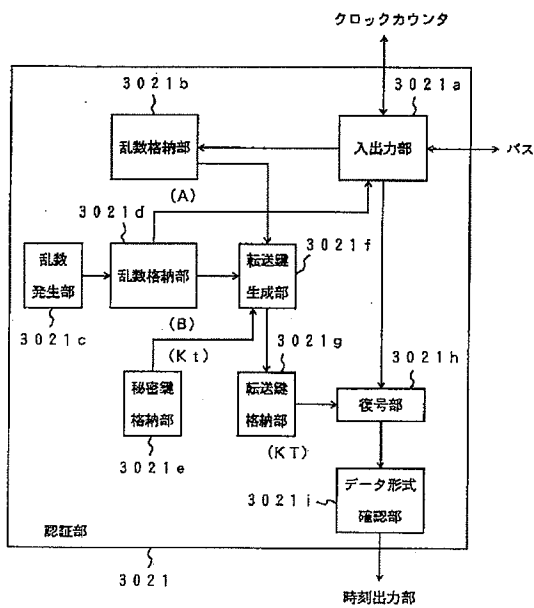
【図77】



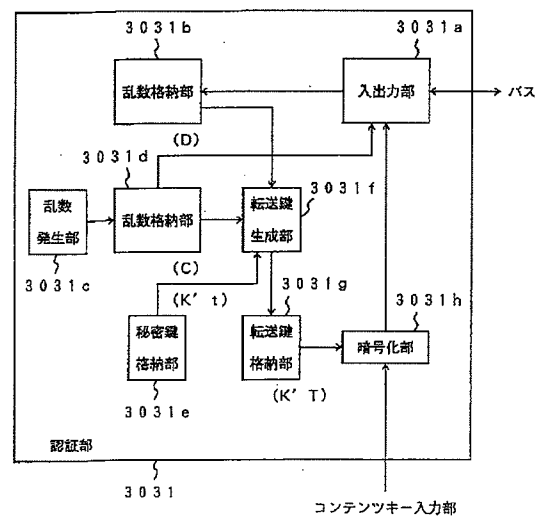
【図79】



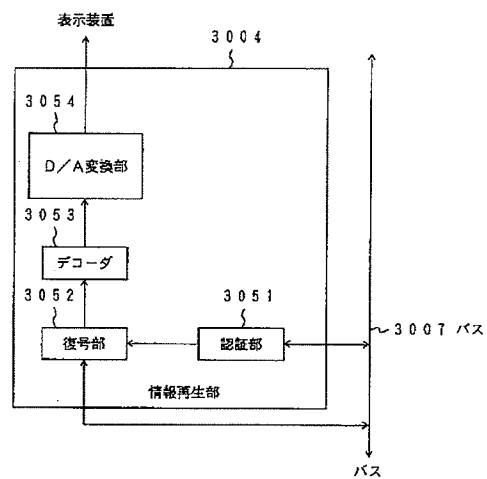
【図82】



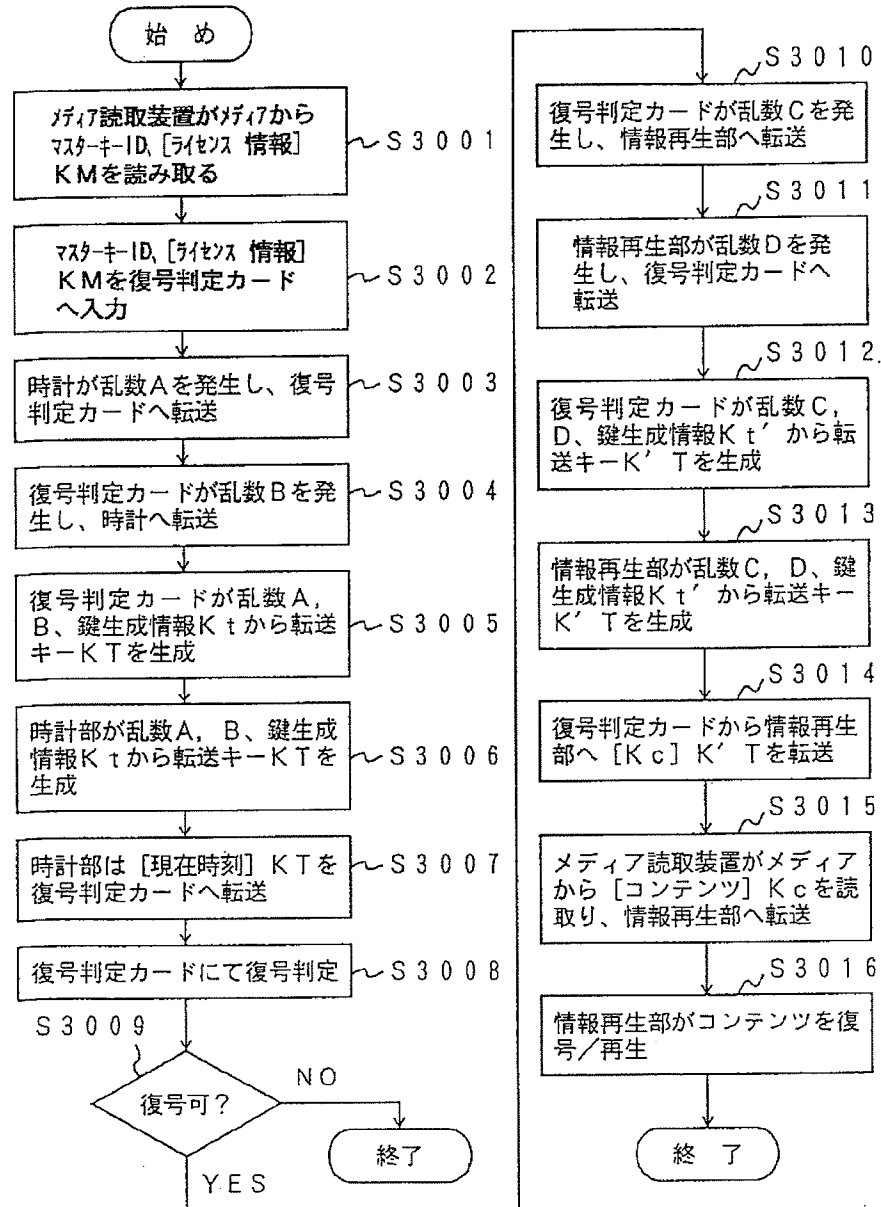
【図85】



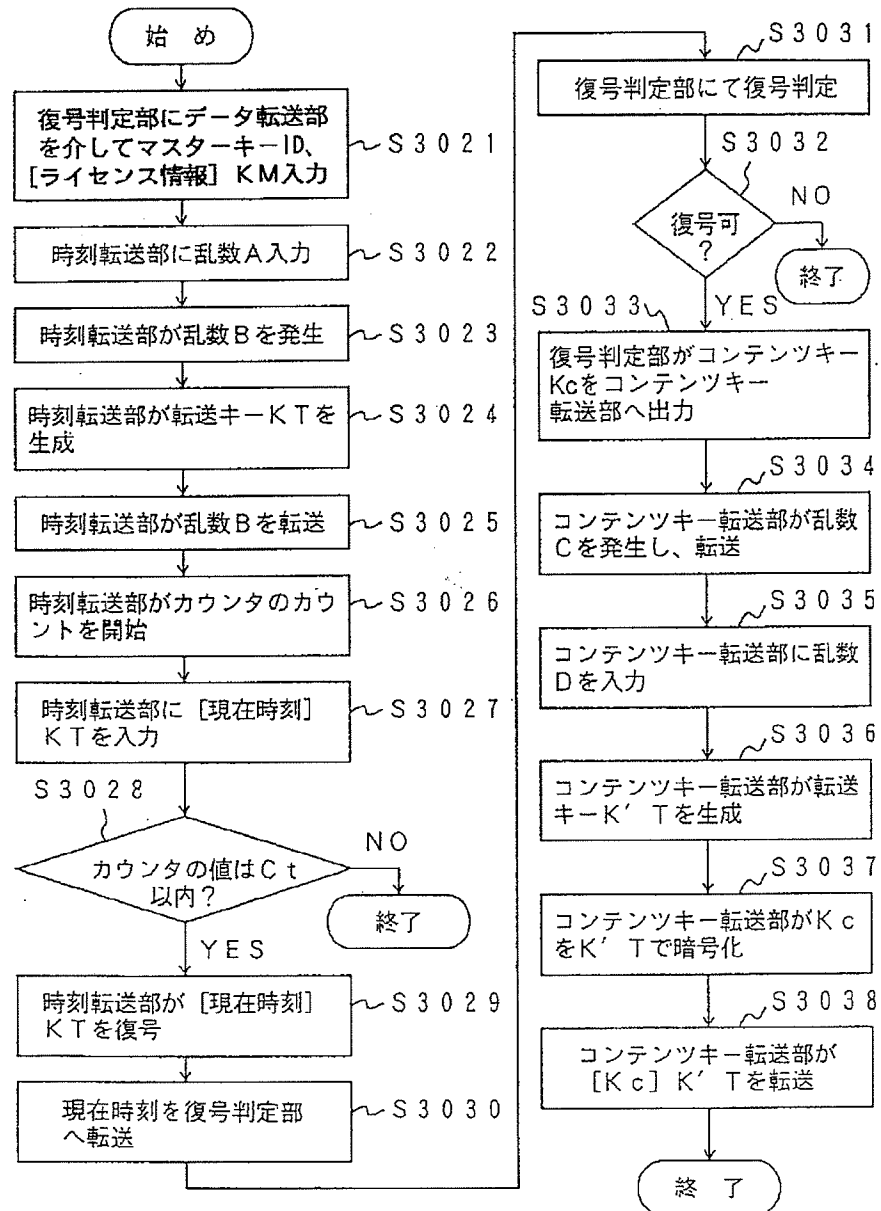
【図92】



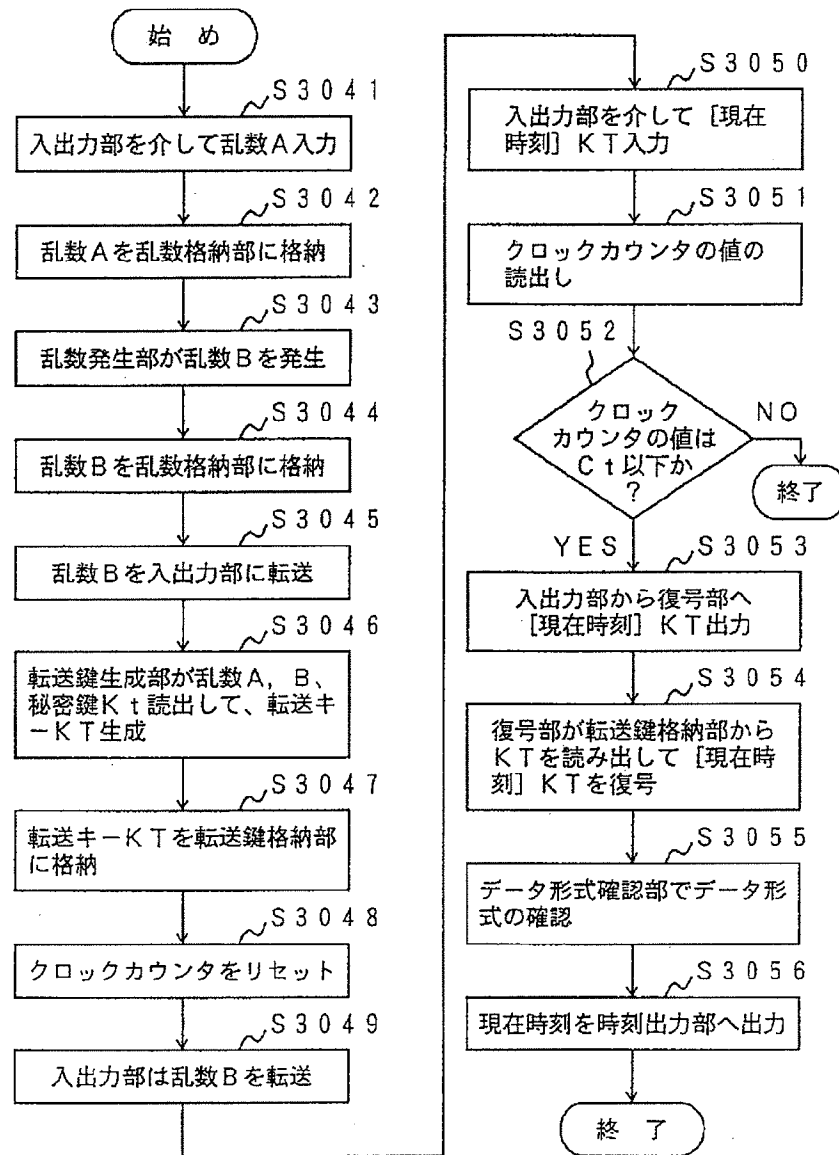
【図78】



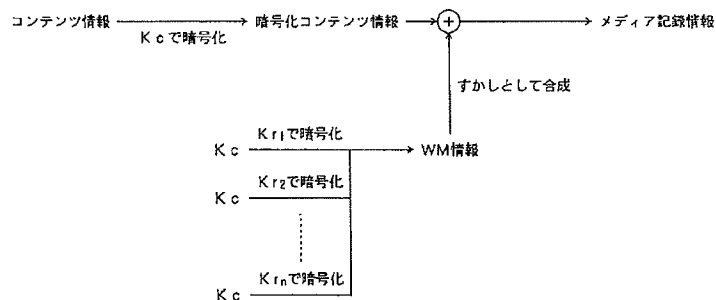
【図80】



【図83】

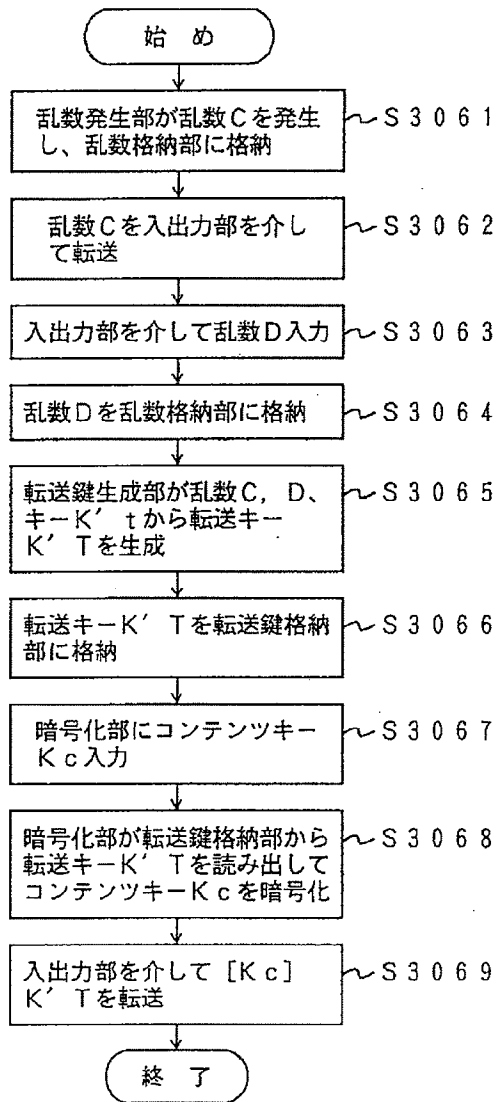


【図170】

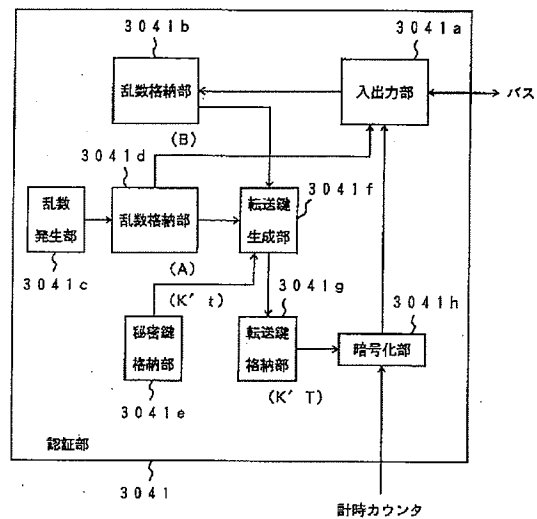




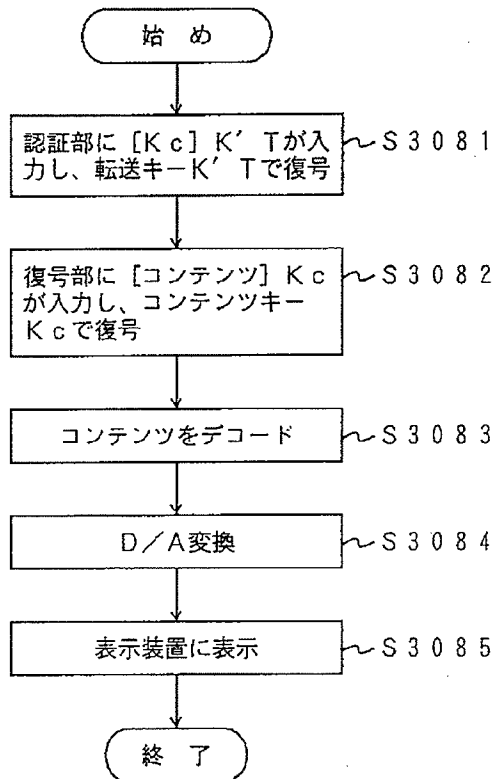
【図86】



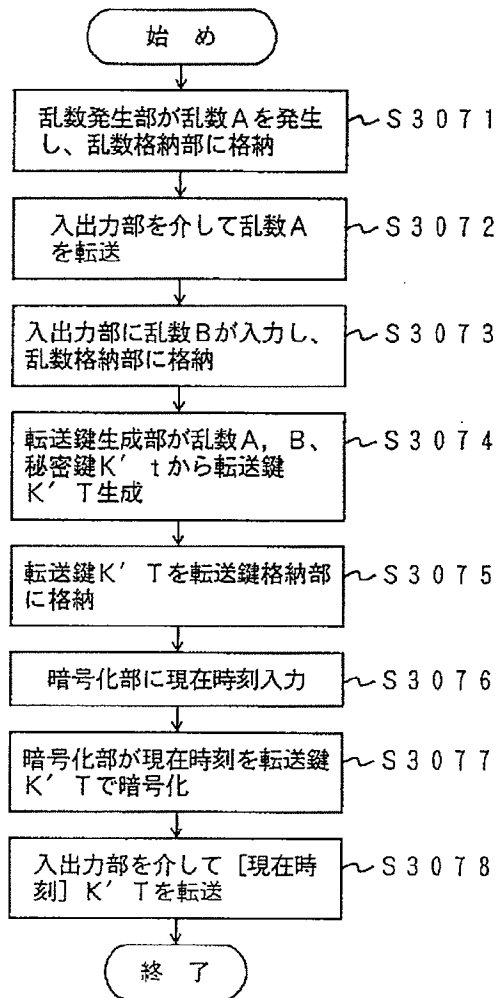
【図88】



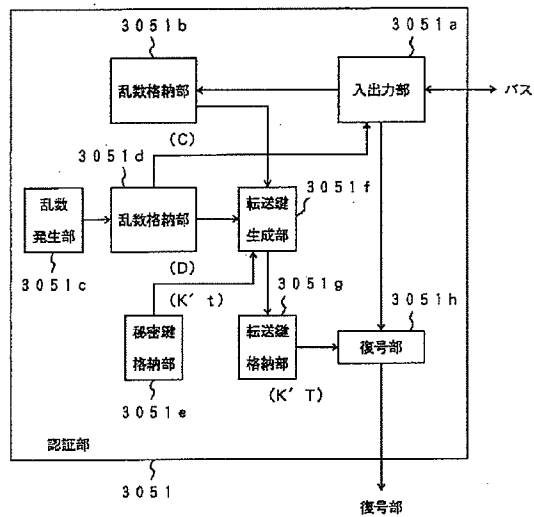
【図93】



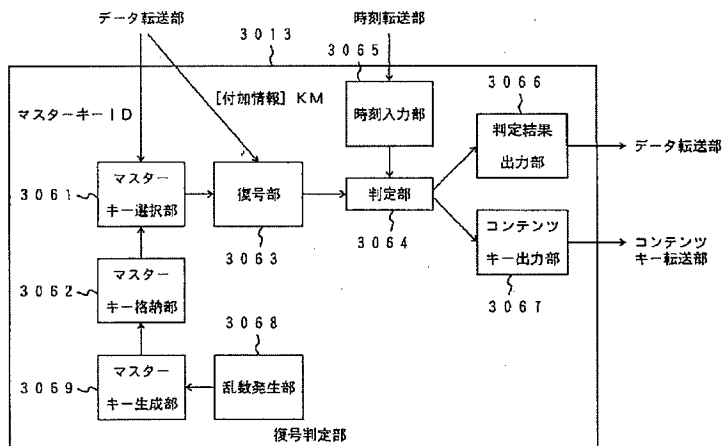
【図89】



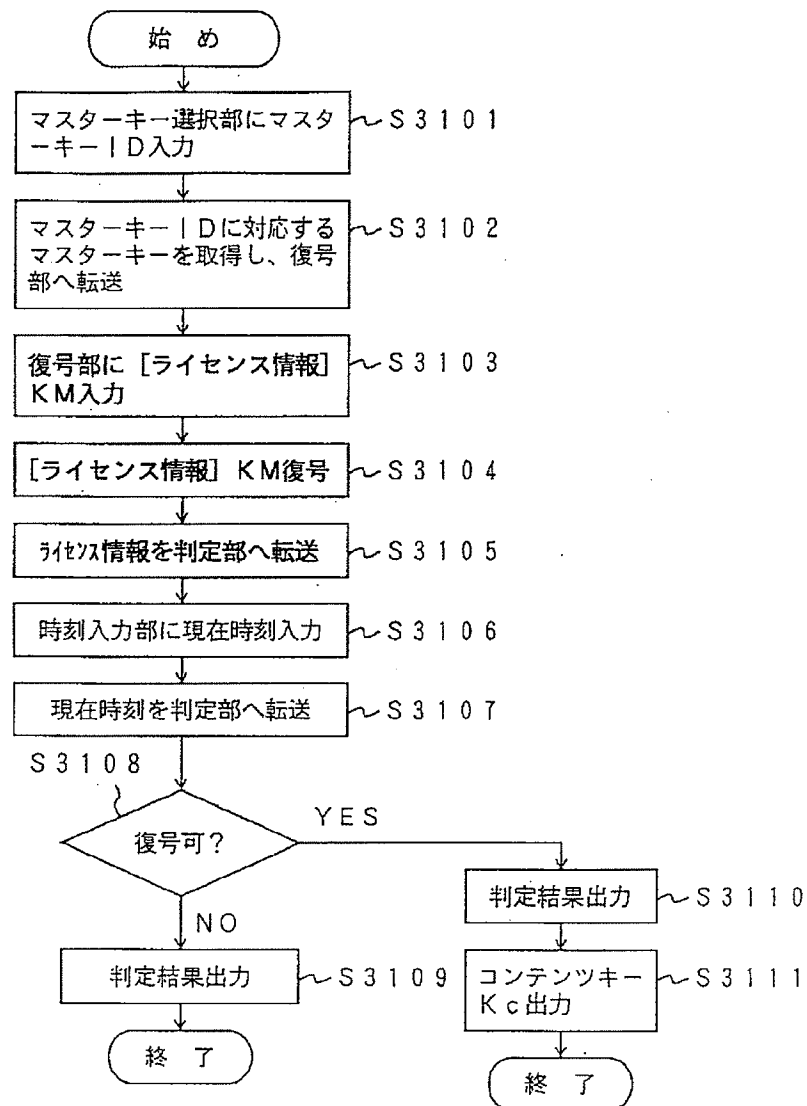
【図94】



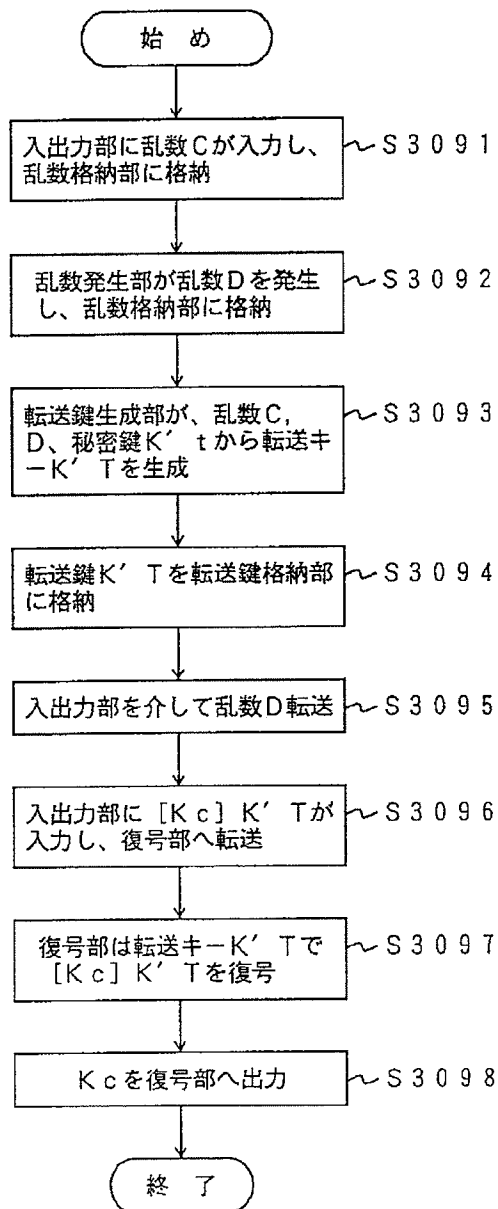
【図90】



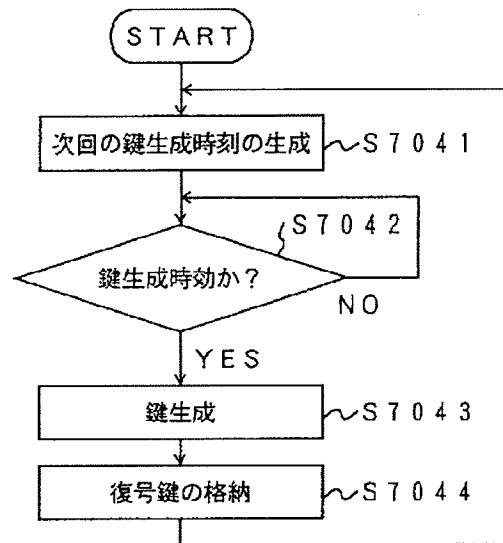
【図91】



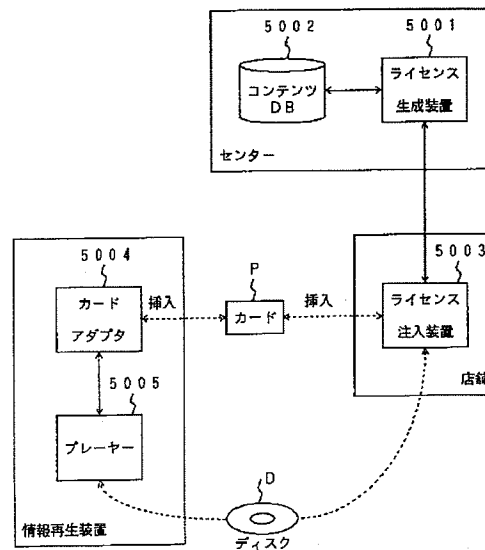
【図95】



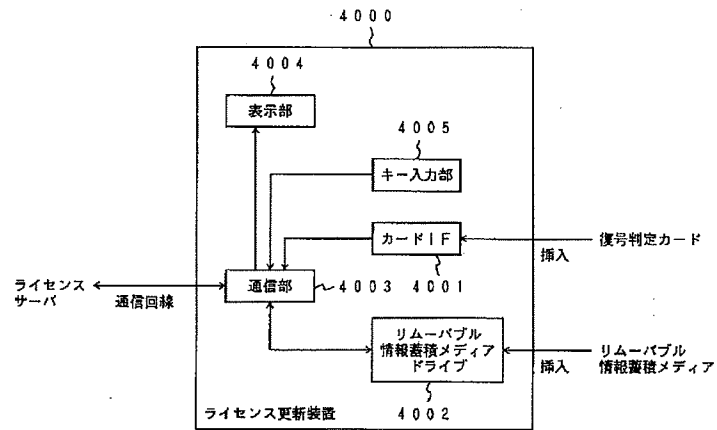
【図112】



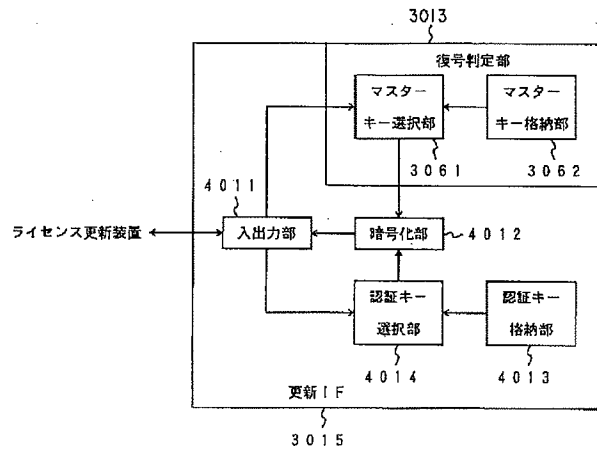
【図122】



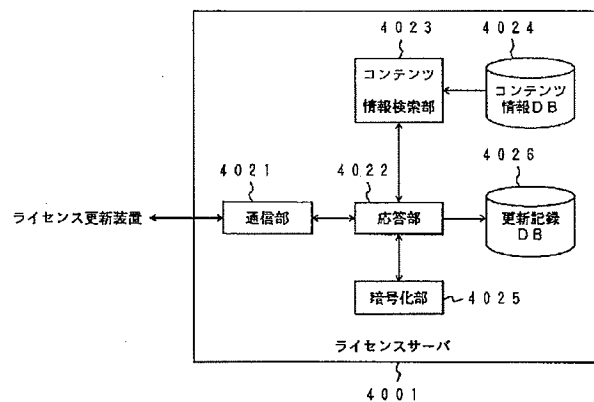
【図97】



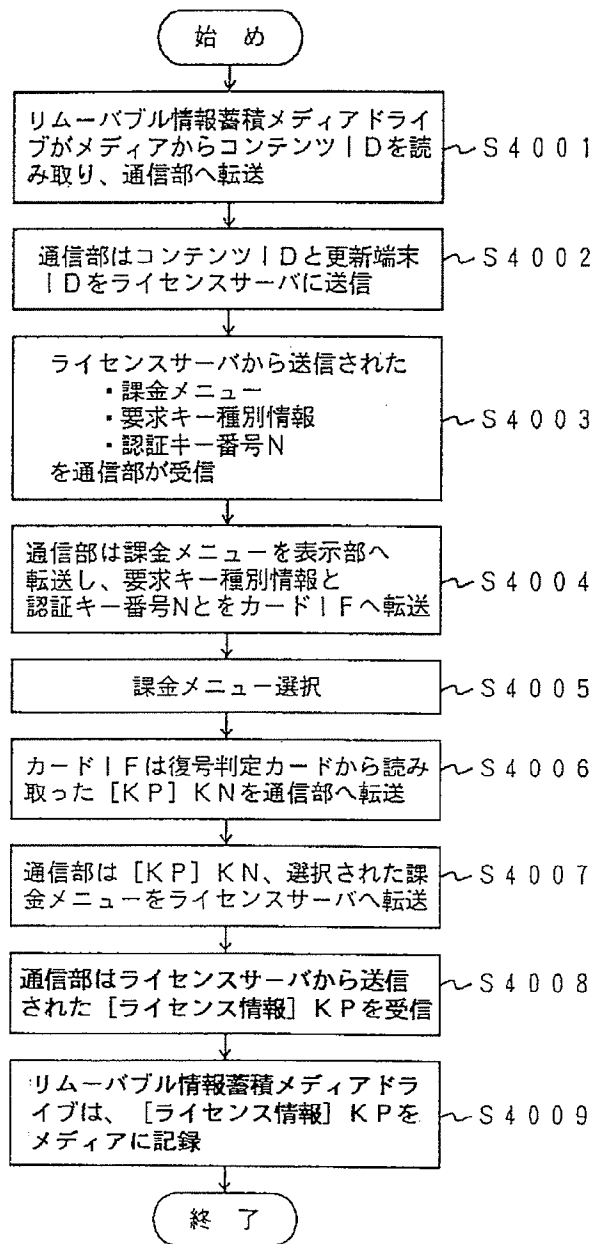
【図99】



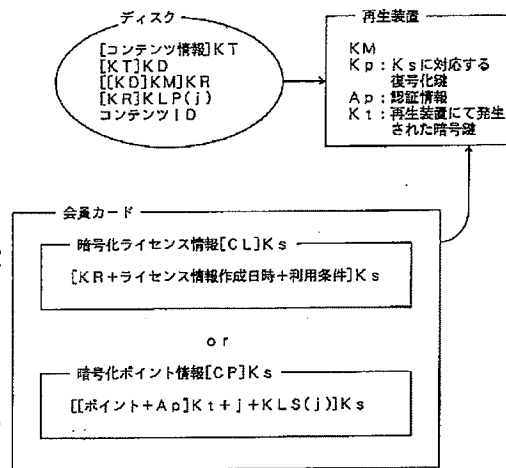
【図101】



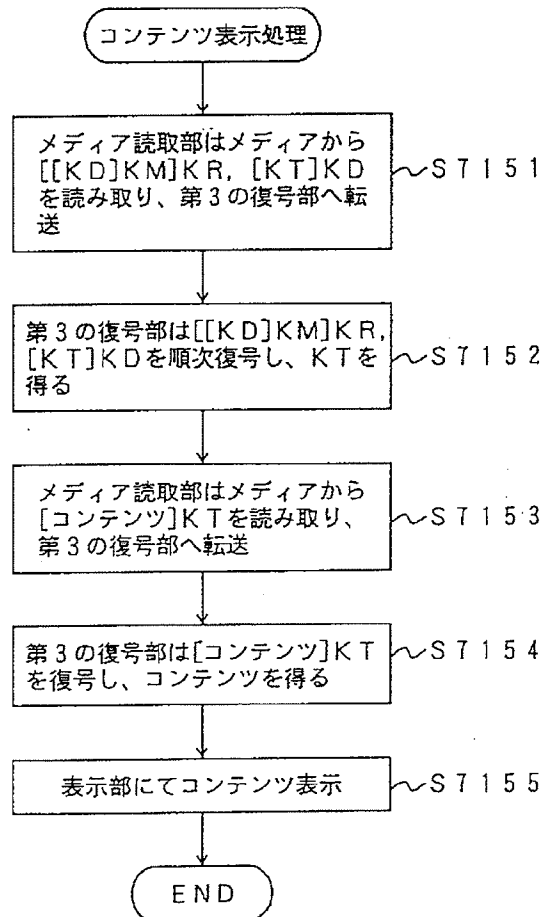
【図98】



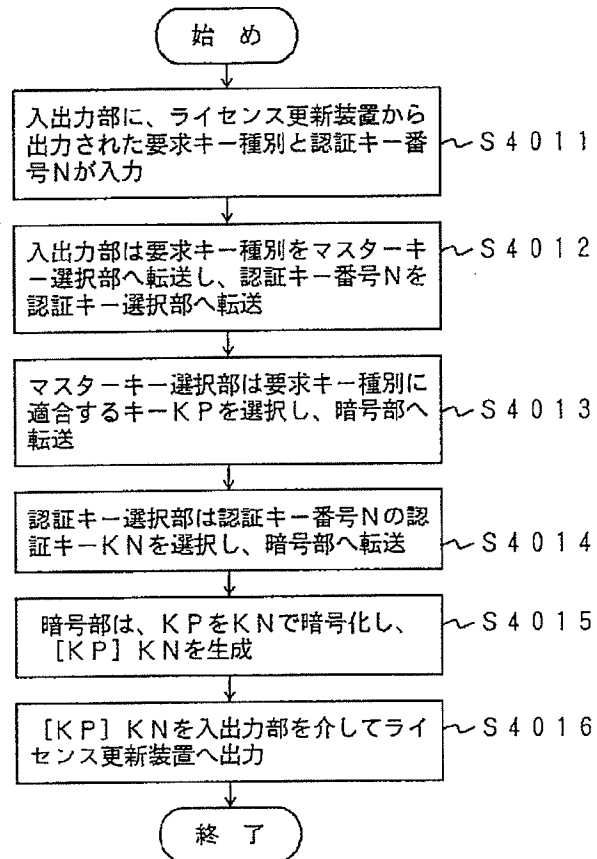
【図151】



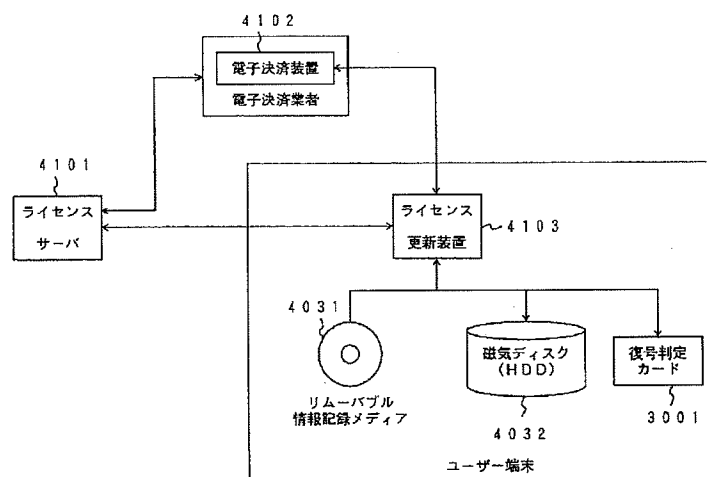
【図157】



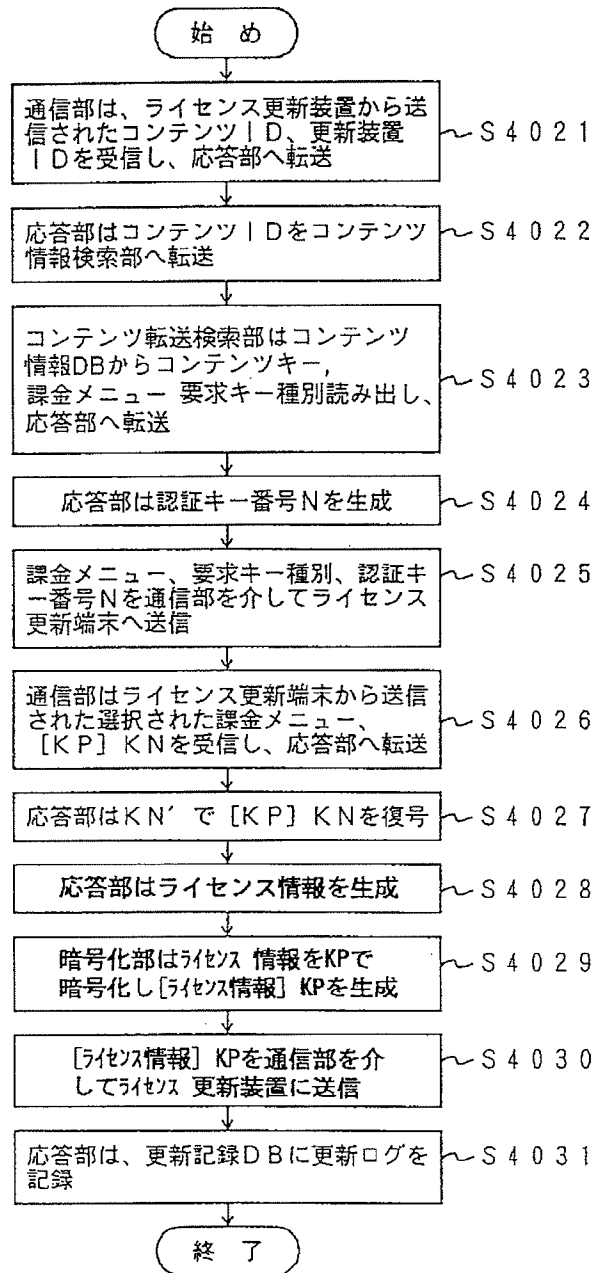
【図100】



【図103】



【図102】





4103

ライセンス更新装置

4045 表示部

4046 入力部

4041 通信部

4044 制御部

4043 復号判定カード IF

3001 復号判定カード

ライセンスサーバ

電子決済装置

4042 リムーバブル情報記録メディア IF

4032 HDD

4031 リムーバブル情報記録メディア

Detailed description: This block diagram illustrates the internal architecture of the license update device 4103. The device is enclosed in a rectangular box labeled 'ライセンス更新装置' (License Update Device) with reference numeral 4103. Inside, a central '制御部' (Control Unit) 4044 is connected to several components: a '表示部' (Display Unit) 4045 and an '入力部' (Input Unit) 4046 at the top; a '通信部' (Communication Unit) 4041 on the left, which connects to a 'ライセンスサーバ' (License Server) outside the device; a '復号判定カード IF' (Decryption Judgment Card Interface) 4043 on the right, which connects to a '復号判定カード' (Decryption Judgment Card) 3001; a 'リムーバブル情報記録メディア IF' (Removable Information Recording Media Interface) 4042 at the bottom, which connects to a 'リムーバブル情報記録メディア' (Removable Information Recording Media) 4031; and an 'HDD' (Hard Disk Drive) 4032. Bidirectional arrows indicate data flow between the control unit and the communication, card interface, media interface, and HDD units.

```

graph LR
    4101[4101 ライセンスサーバ]
    4051[4051 通信部]
    4052[4052 復号部]
    4053[4053 例部]
    4054[4054 課金処理番号発行部]
    4055[4055 課金処理部]
    4056[4056 ライセンス情報生成部]
    4057[(4057 課金処理DB)]
    4058[(4058 課金DB)]

    4051 --> LicenseUpdate[ライセンス更新装置]
    4051 <--> 4052
    4052 --> 4053
    4053 --> 4054
    4053 --> 4056
    4054 --> 4058
    4056 --> 4058
    4055 <--> 4057
    4055 <--> 4058
  
```

Figure 1 is a block diagram of a license server (4101). The server includes a communication unit (4051), a restoration unit (4052), an example unit (4053), a license information generation unit (4056), a license number issuance unit (4054), a license processing unit (4055), a license DB (4057), and a license DB (4058). The communication unit (4051) is connected to a license update device. The restoration unit (4052) is connected to the communication unit (4051) and the example unit (4053). The example unit (4053) is connected to the license information generation unit (4056) and the license number issuance unit (4054). The license information generation unit (4056) is connected to the license DB (4058). The license number issuance unit (4054) is connected to the example unit (4053) and the license DB (4058). The license processing unit (4055) is connected to the license DB (4057) and the license DB (4058).

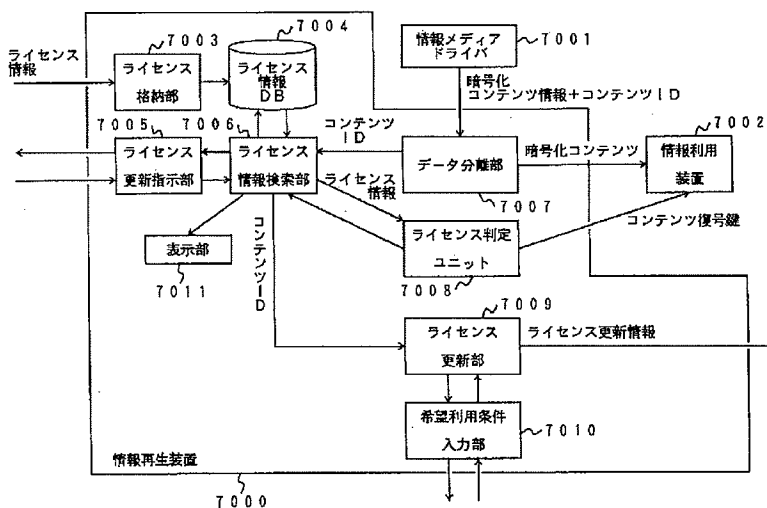
The diagram illustrates the system configuration and data flow. It is divided into four main functional areas by vertical dashed lines:

- ディスク (D I D):** Contains a **プレーヤー** (Player) component. It receives data  $X(D), AD(PD), PrD$  and  $ksD$  from the Card area and outputs  $[ディスクキー]w_2$  to the Disk Key component.
- カードアダプタ (A I D):** Contains a **カード** (Card) component. It receives data  $X(I), A(I(P1)), PrI$  and  $X(k), Ak(Pk), Prk$  from the License area. It outputs  $ksD$  to the Disk area and  $[ライセンス情報]w_2$  to the License Creation area.
- ライセンス:** Contains a **注入装置** (Injection Device) component. It receives data  $X(I), A(I(P1)), PrI$  and  $X(k), Ak(Pk), Prk$  from the License Creation area. It outputs  $ksL$  to the License Creation area.
- ライセンス作成装置:** Contains a **作成装置** (Creation Device) component. It receives data  $XsD, ksA, ksC, ksL$  from the License area. It outputs  $ksD$  to the Card area and  $[ディスクキー]w_2$  to the Disk Key component.

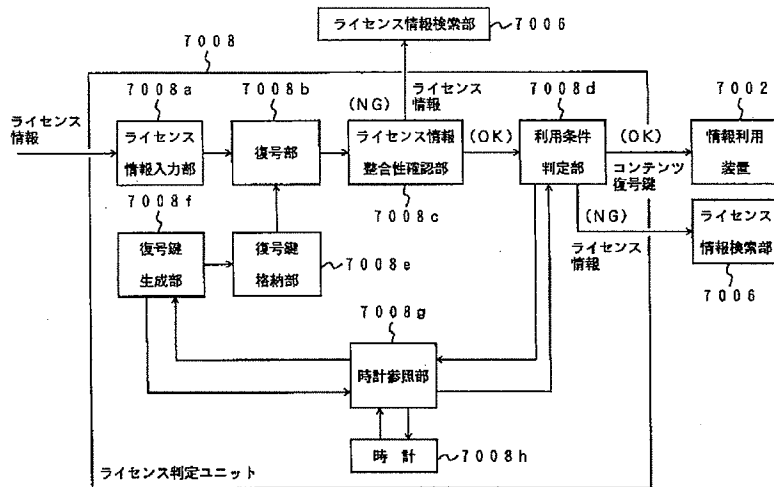
**Data Flow Summary:**

- License Creation to License:**  $X(I), A(I(P1)), PrI$  and  $X(k), Ak(Pk), Prk$  are sent to the License area.
- License to Card Adapter:**  $X(I), A(I(P1)), PrI$  and  $X(k), Ak(Pk), Prk$  are sent to the Card area.
- Card Adapter to Disk Player:**  $X(D), AD(PD), PrD$  and  $ksD$  are sent to the Player.
- License Creation to Disk Key:**  $[ディスクキー]w_2$  is sent to the Disk Key component.
- Disk Key to Card Adapter:**  $[ライセンス情報]w_2$  is sent to the Card area.
- License Creation to License:**  $XsD, ksA, ksC, ksL$  are sent to the License area.
- License to License Creation:**  $ksL$  is sent to the Creation device.
- License Creation to Card Adapter:**  $ksD$  is sent to the Card area.

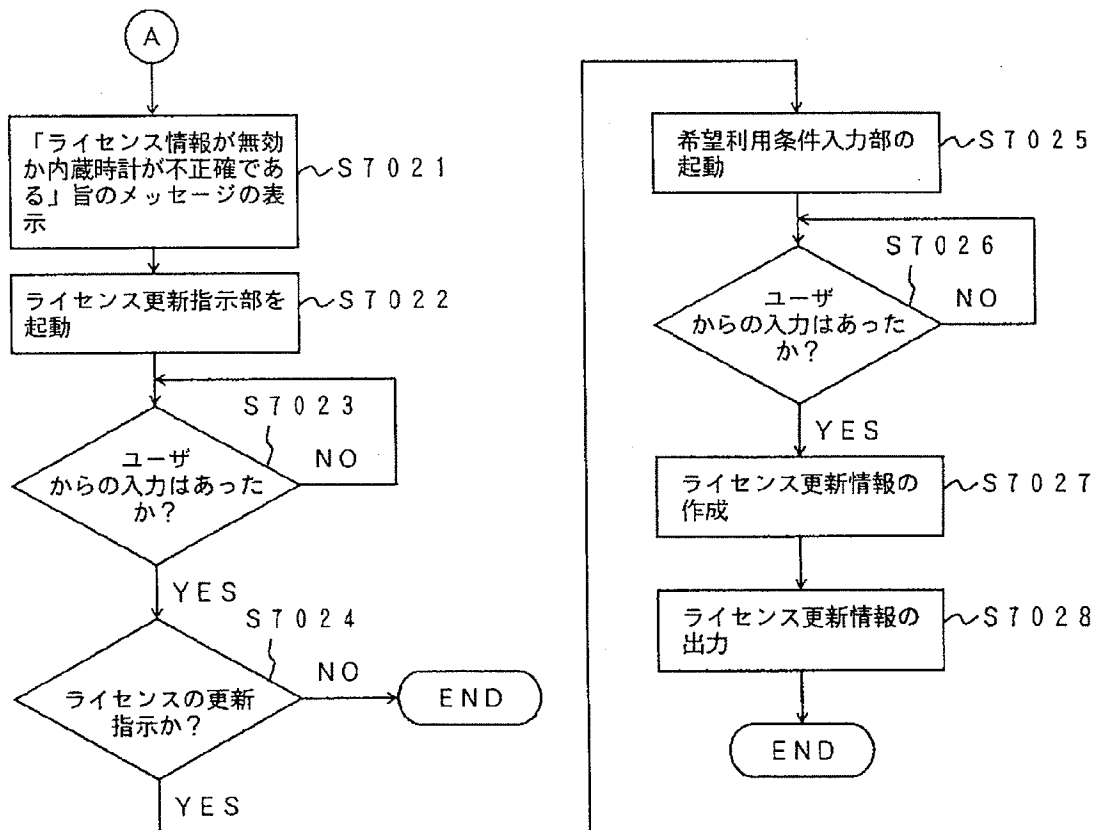
【図107】



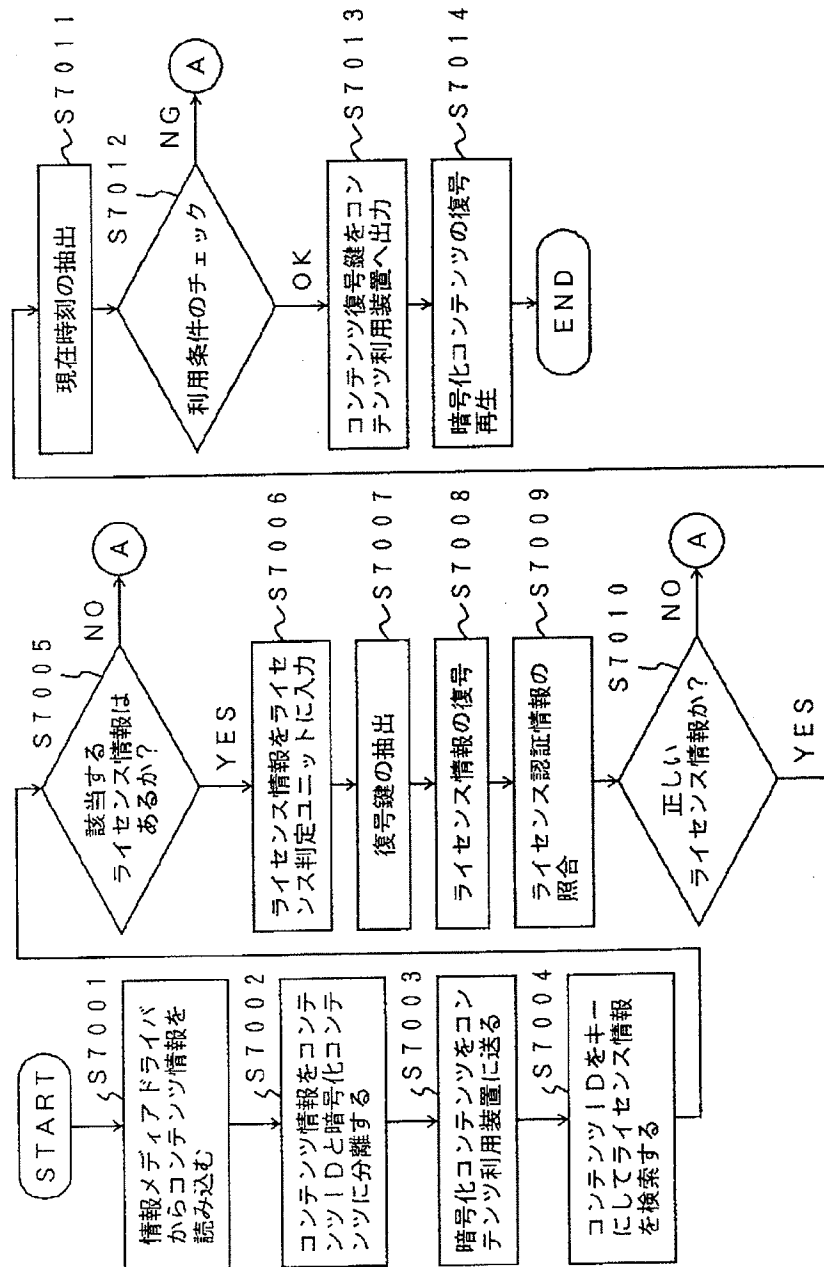
【図108】



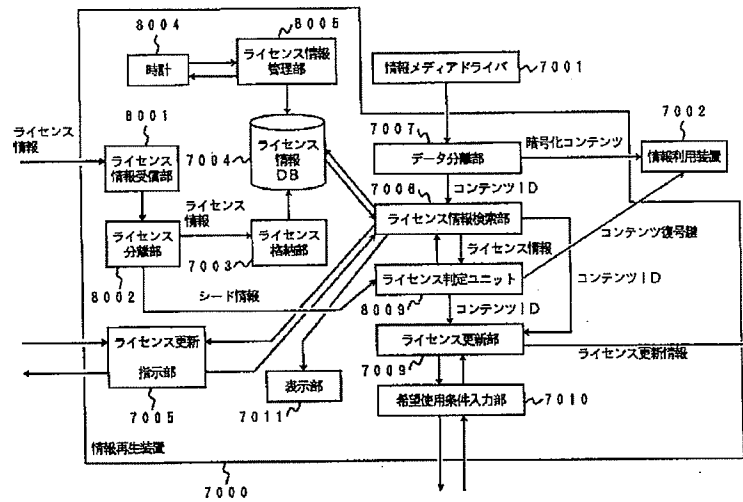
【図 1 1 0】



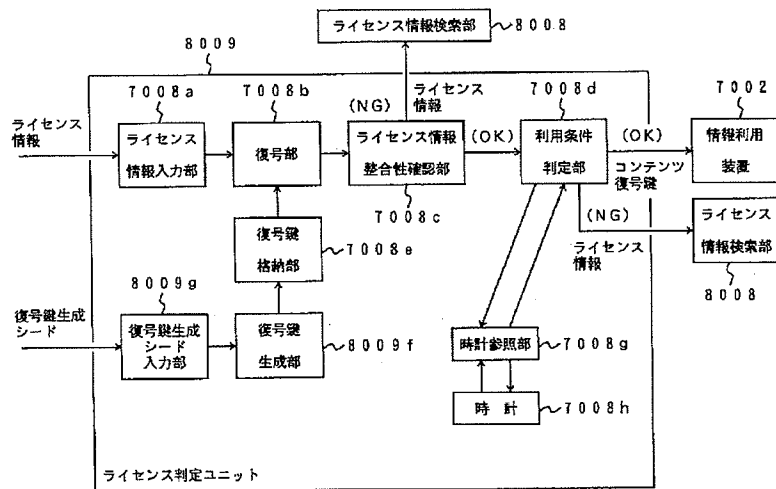
【図109】



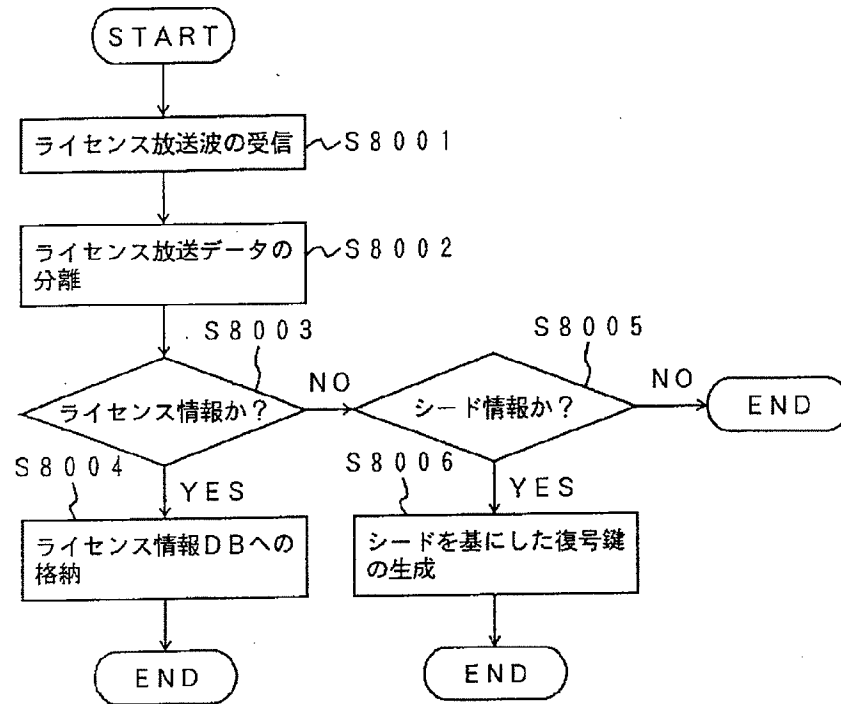
【図118】



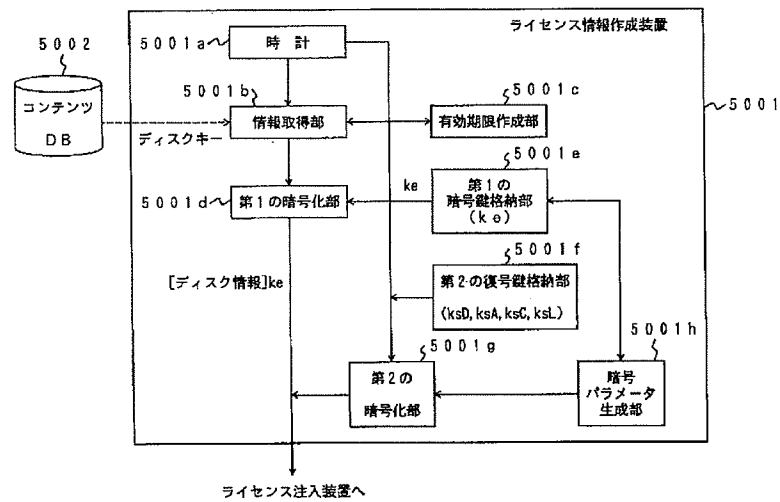
【図119】



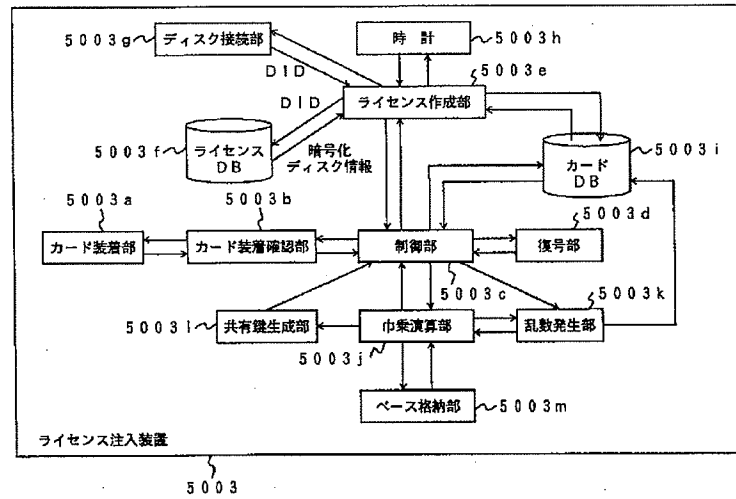
【図120】



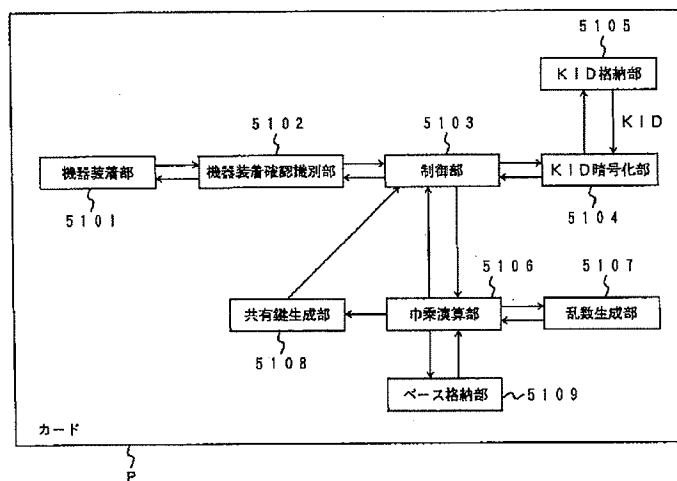
【図126】



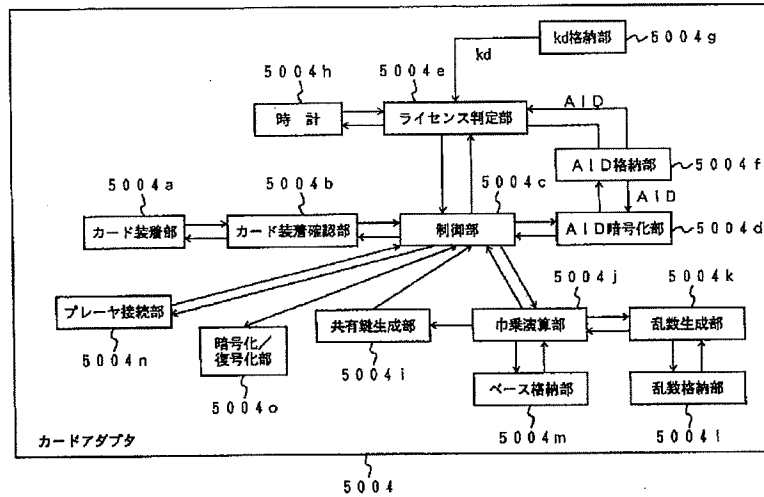
【図127】



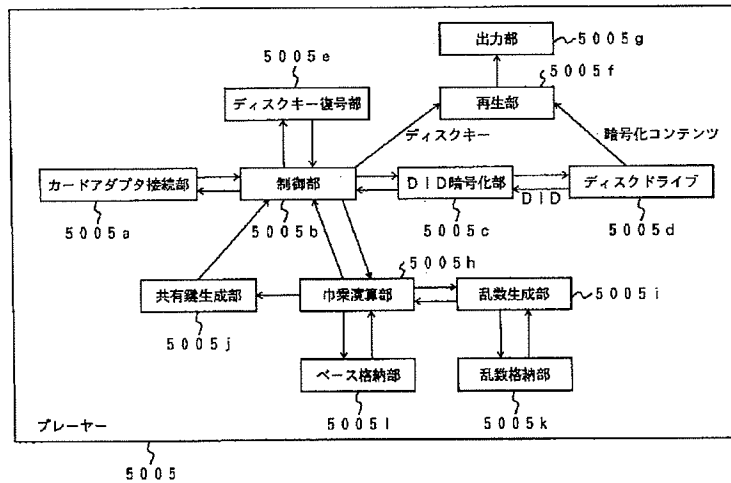
【図128】



【図129】

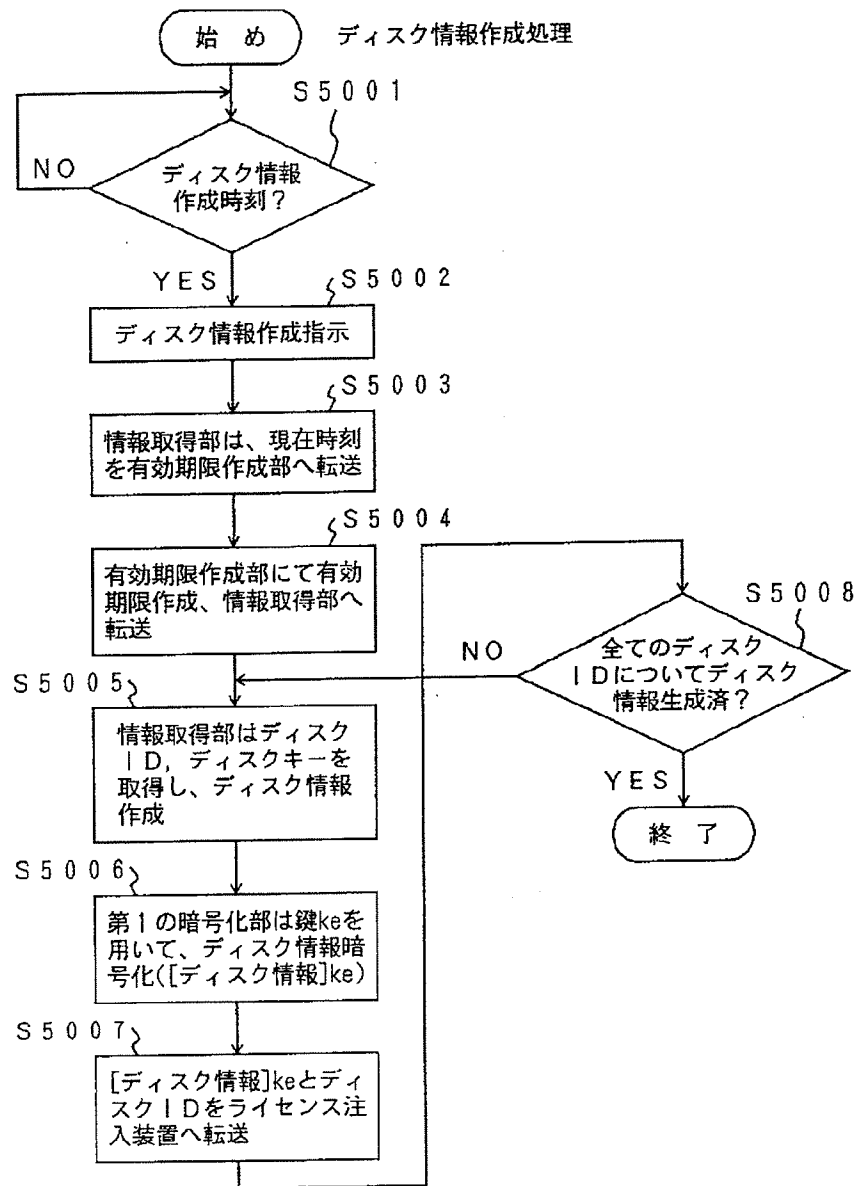


【図130】

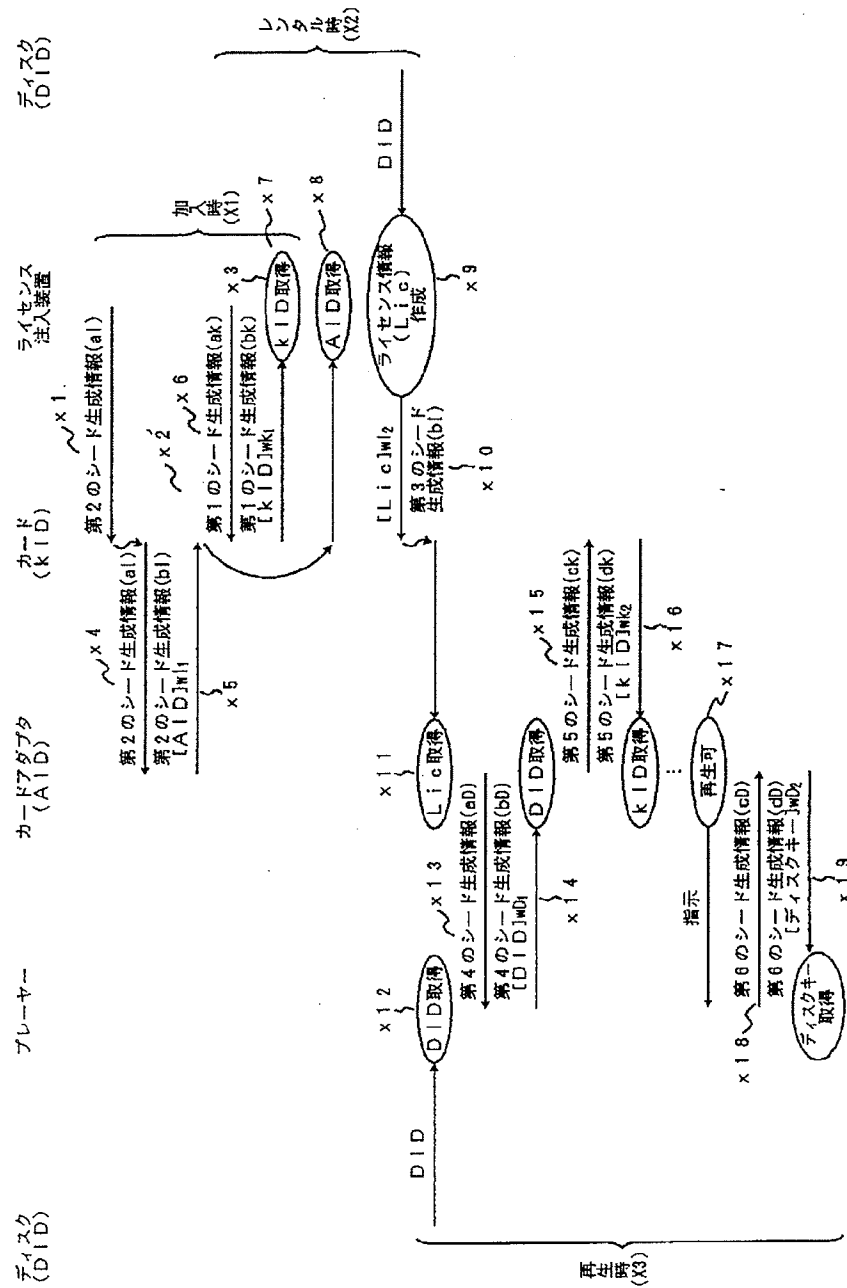




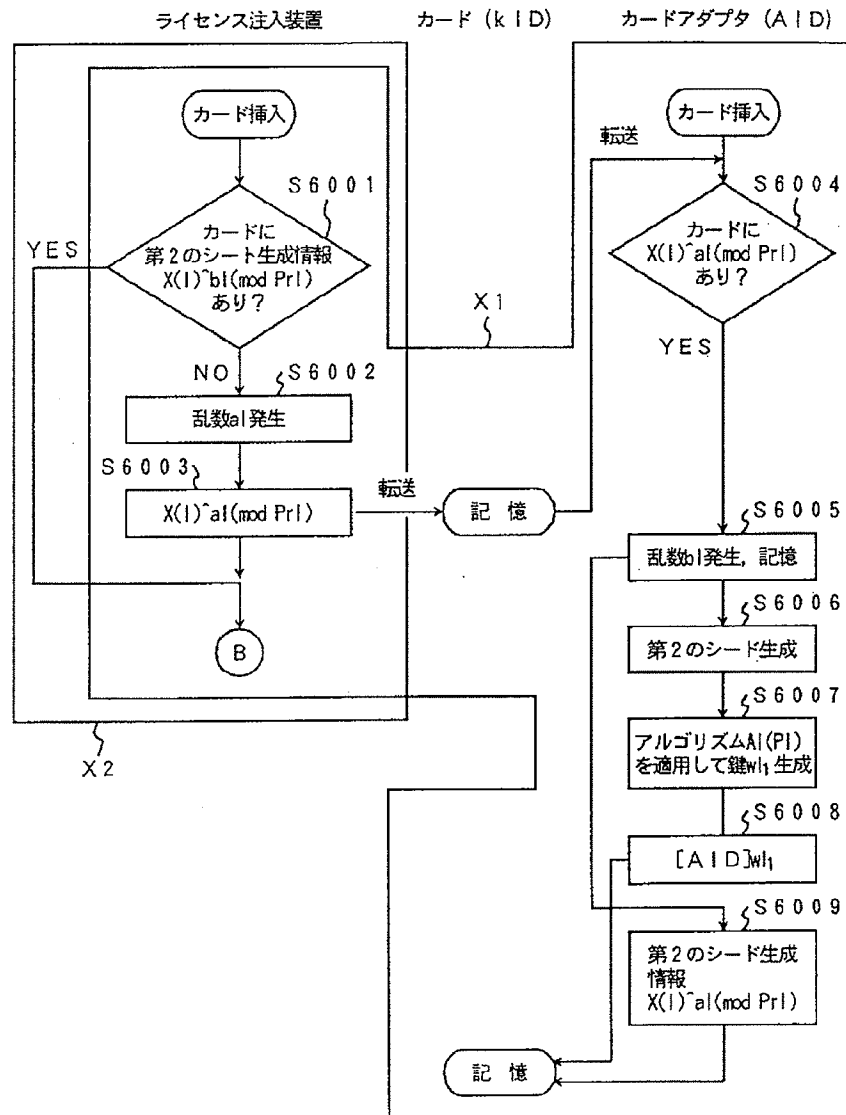
【図131】



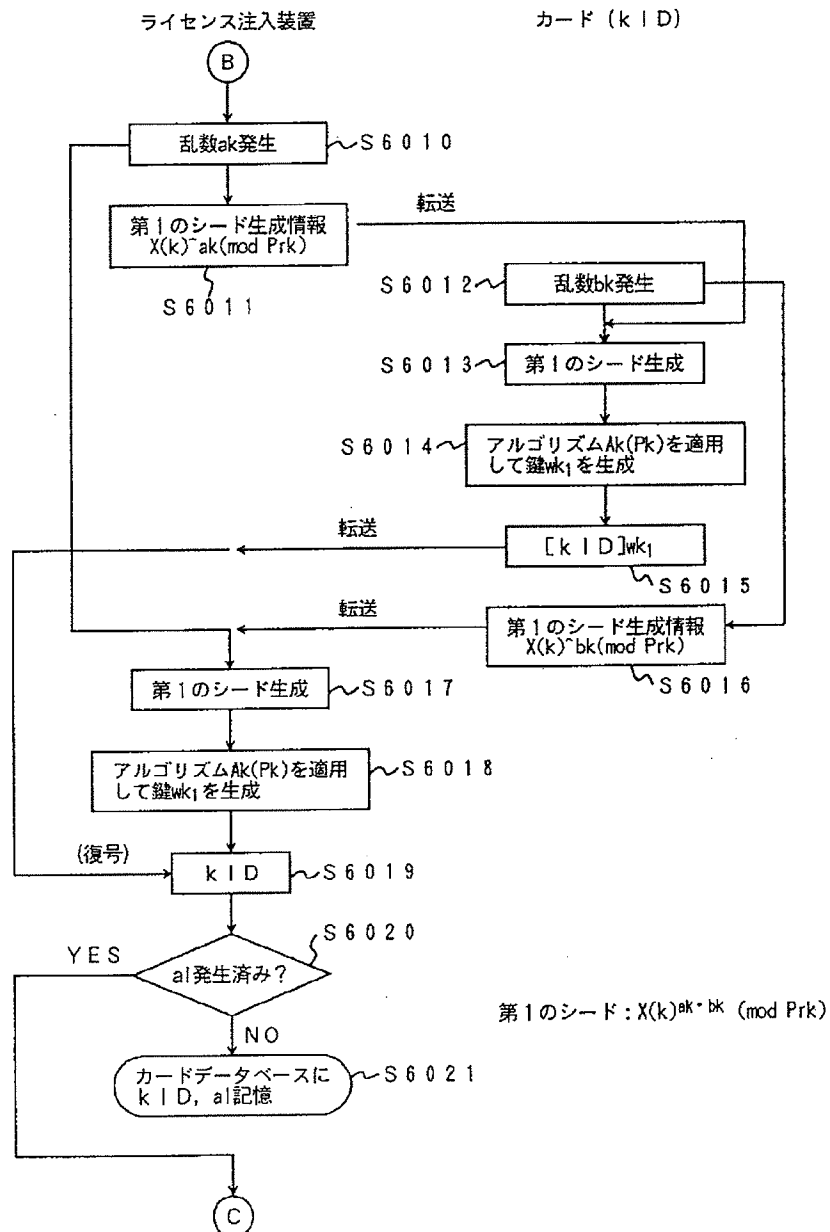
【図133】



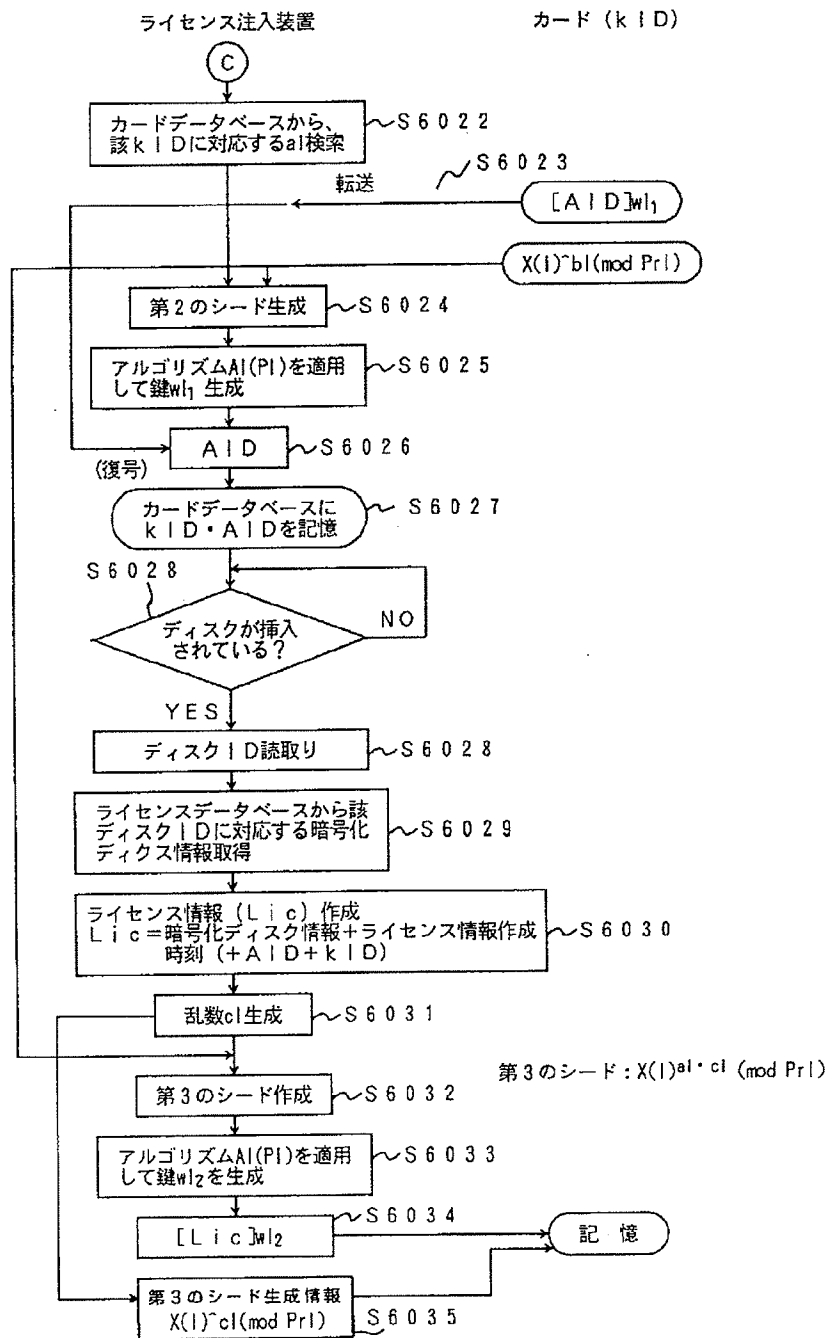
【図134】

第2のシード:  $X(1)^{al \cdot bl} \pmod{Pr1}$

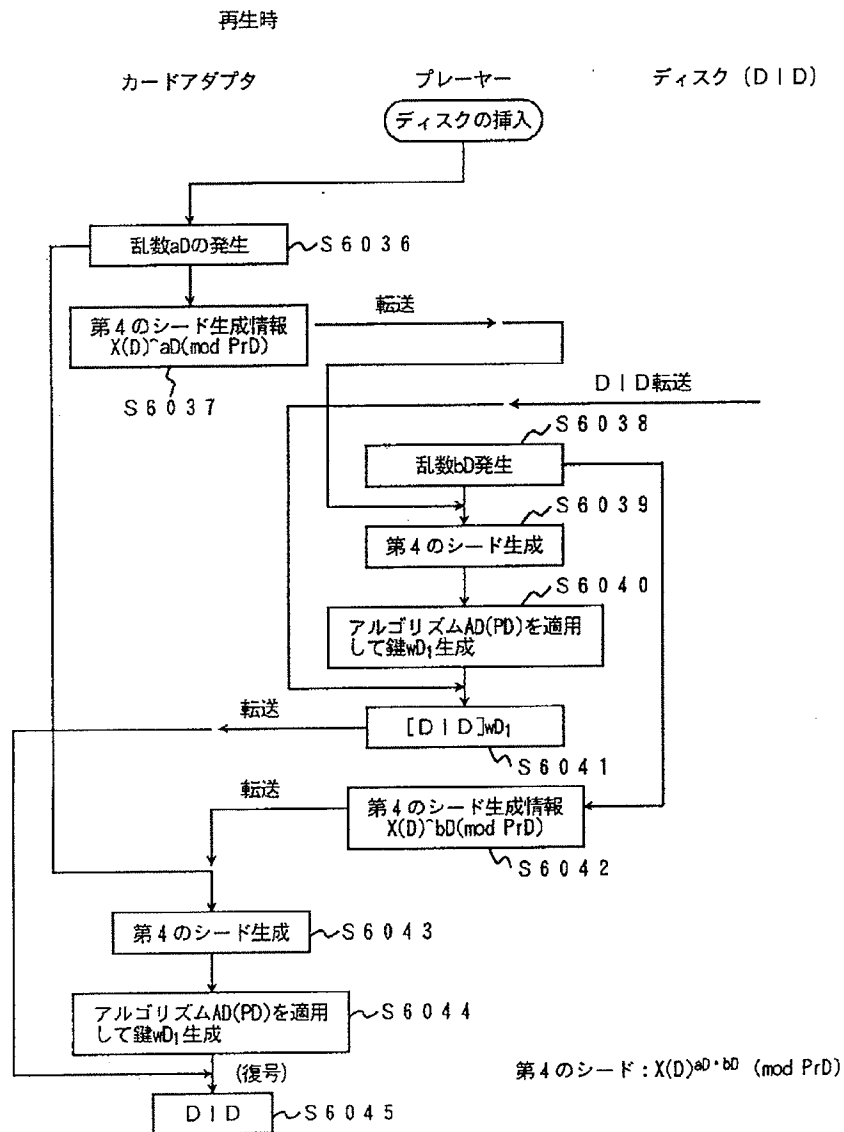
【図135】



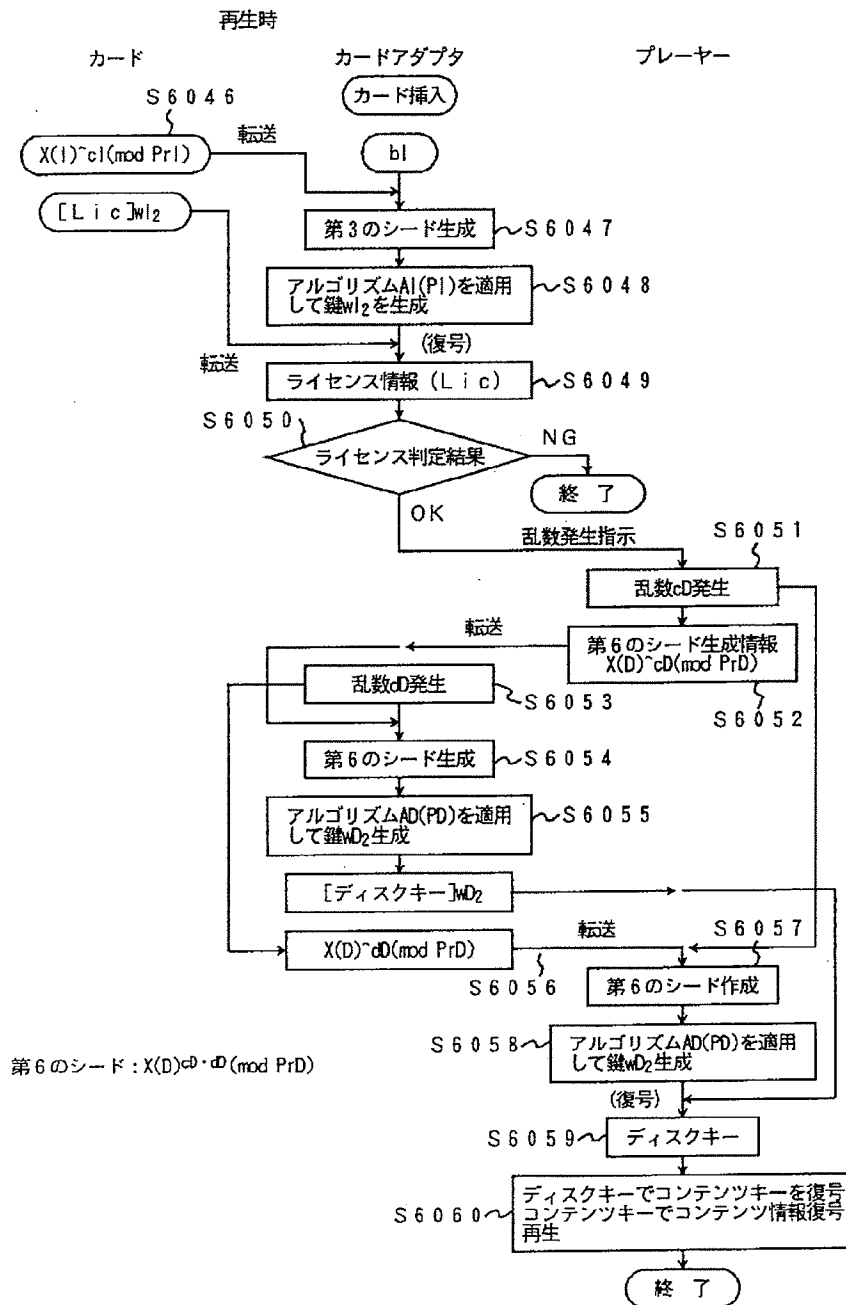
【図136】



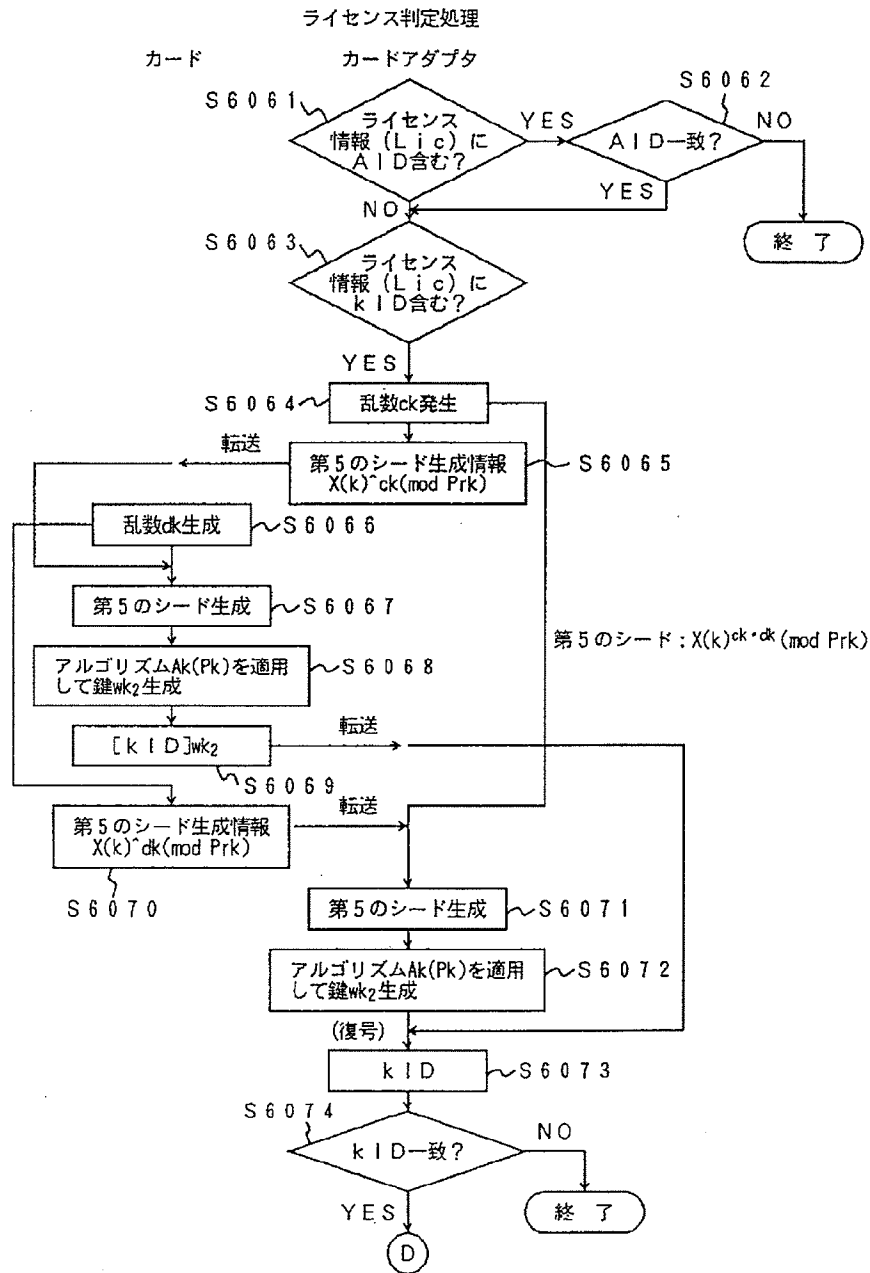
【図137】



【図138】

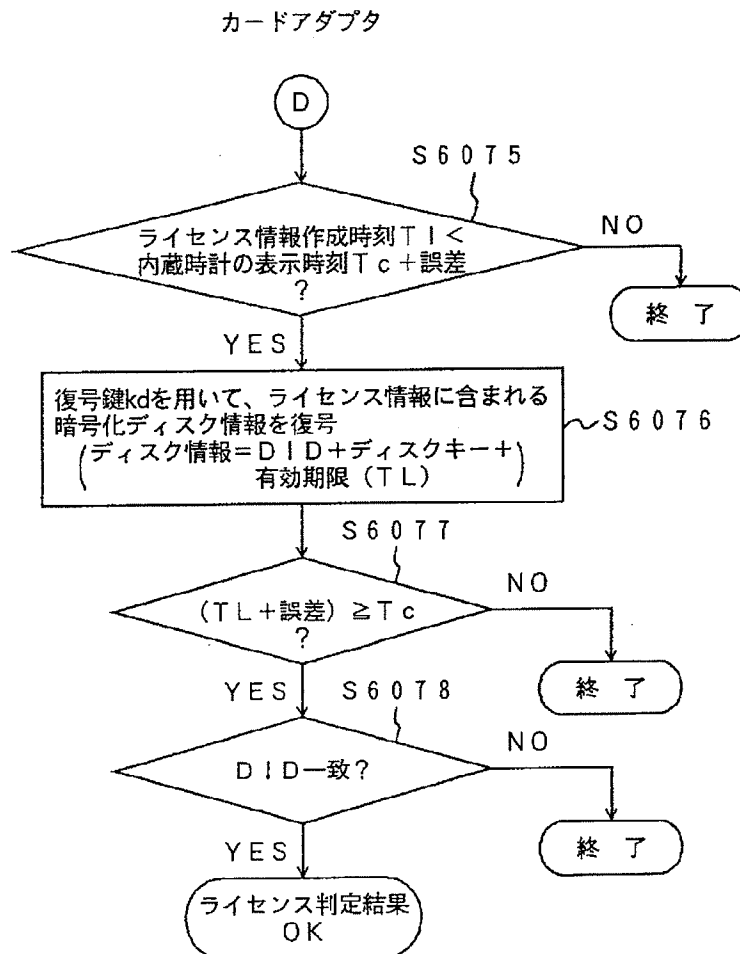


【図139】

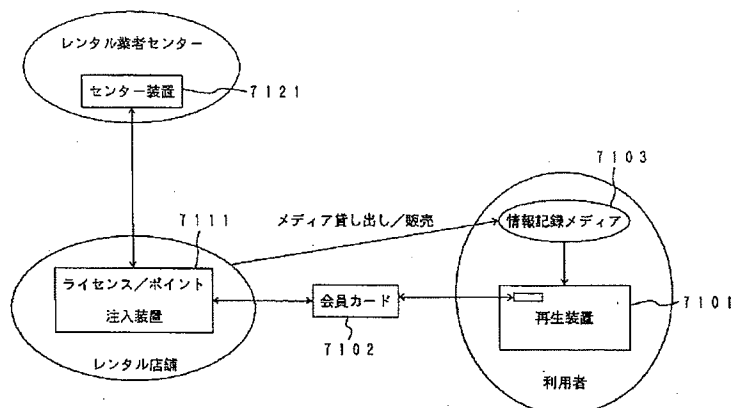




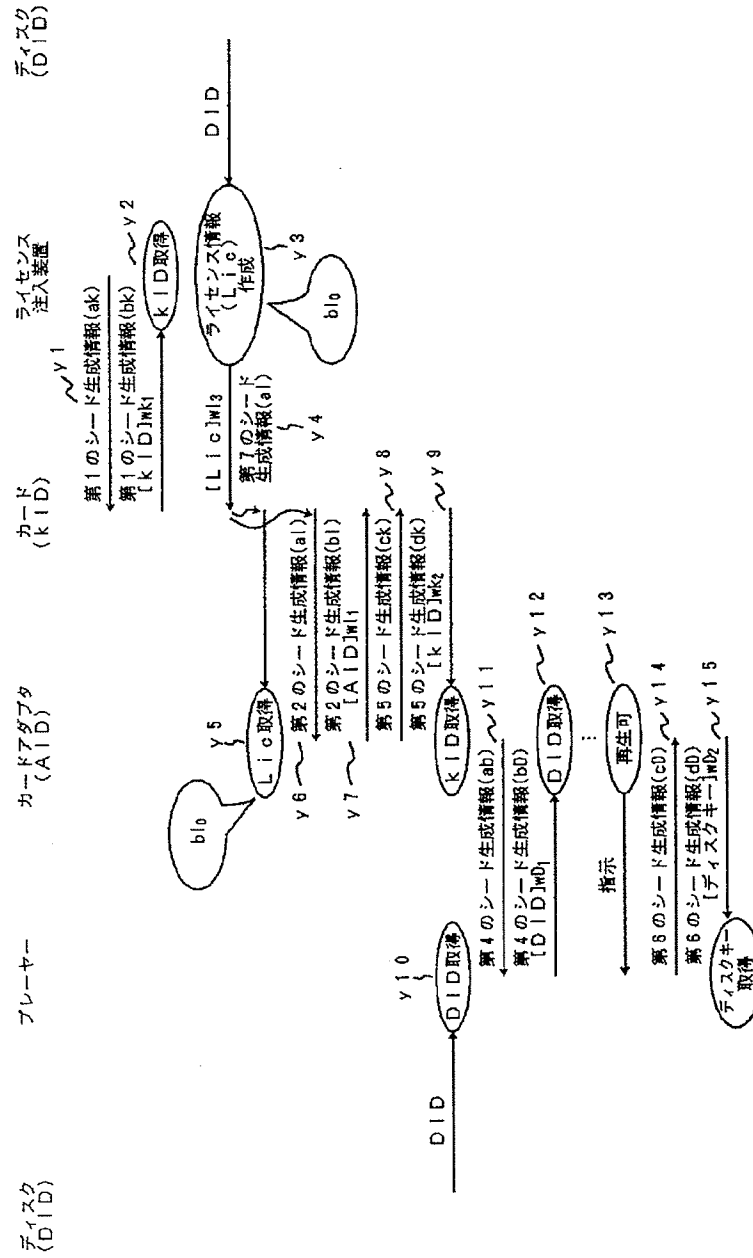
【図140】



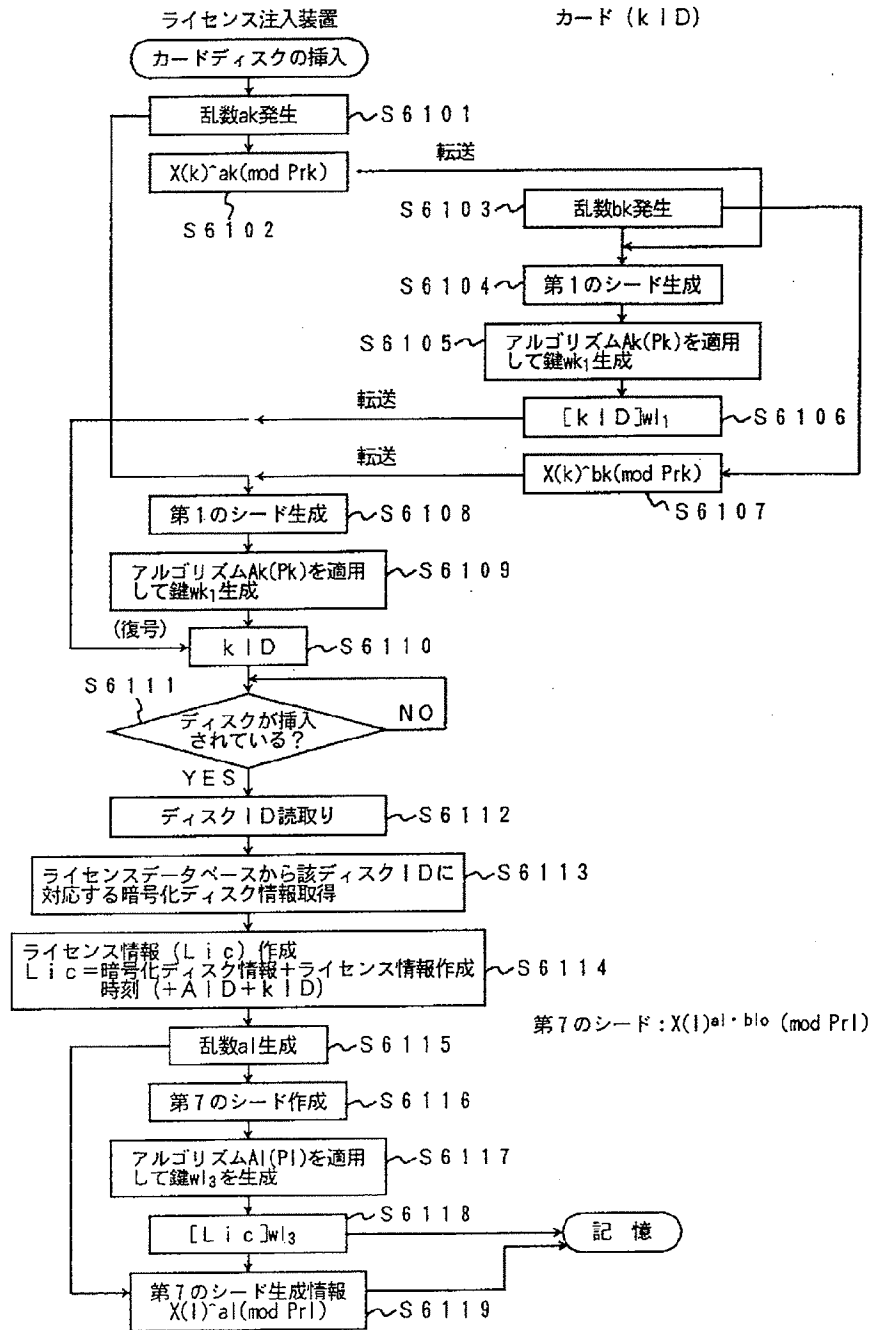
【図150】



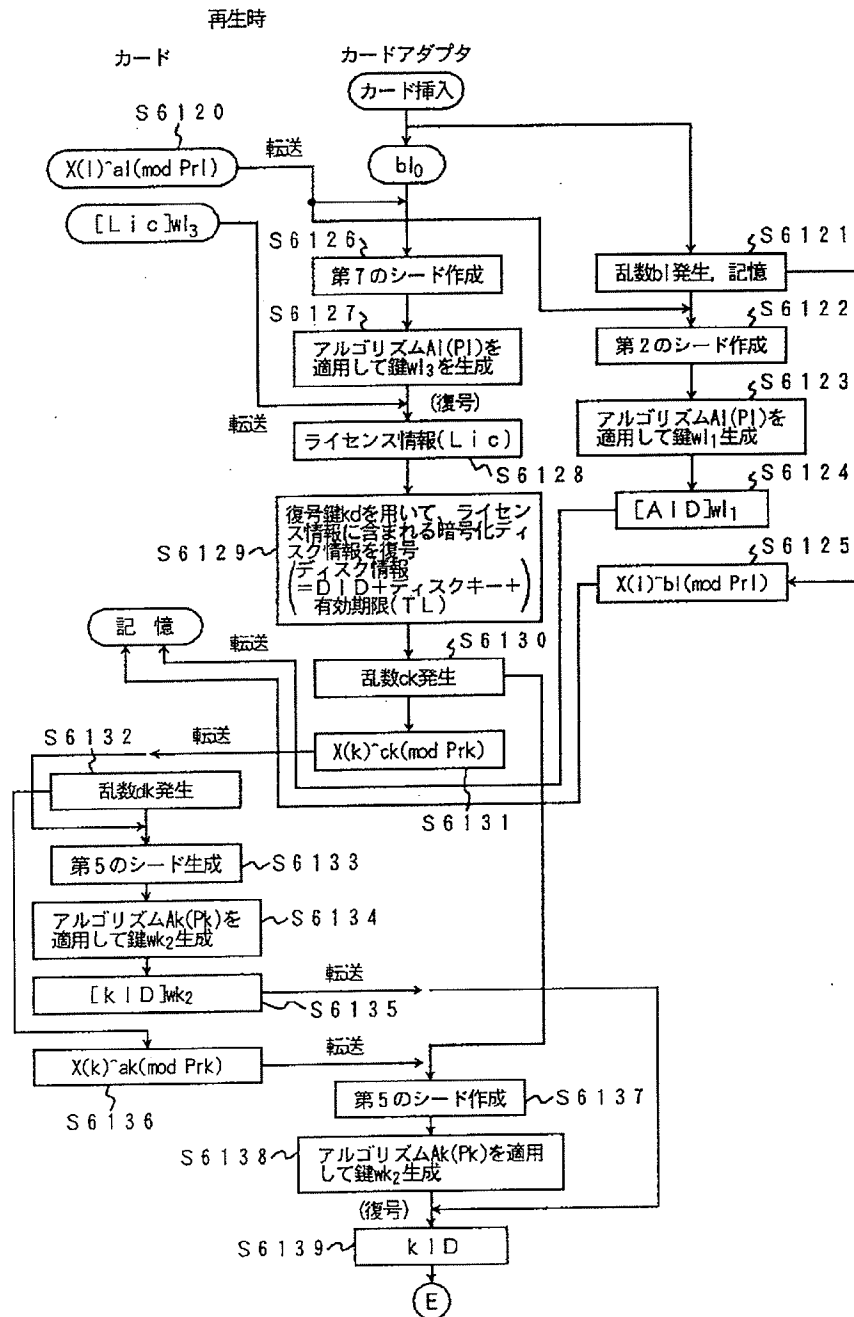
【図141】



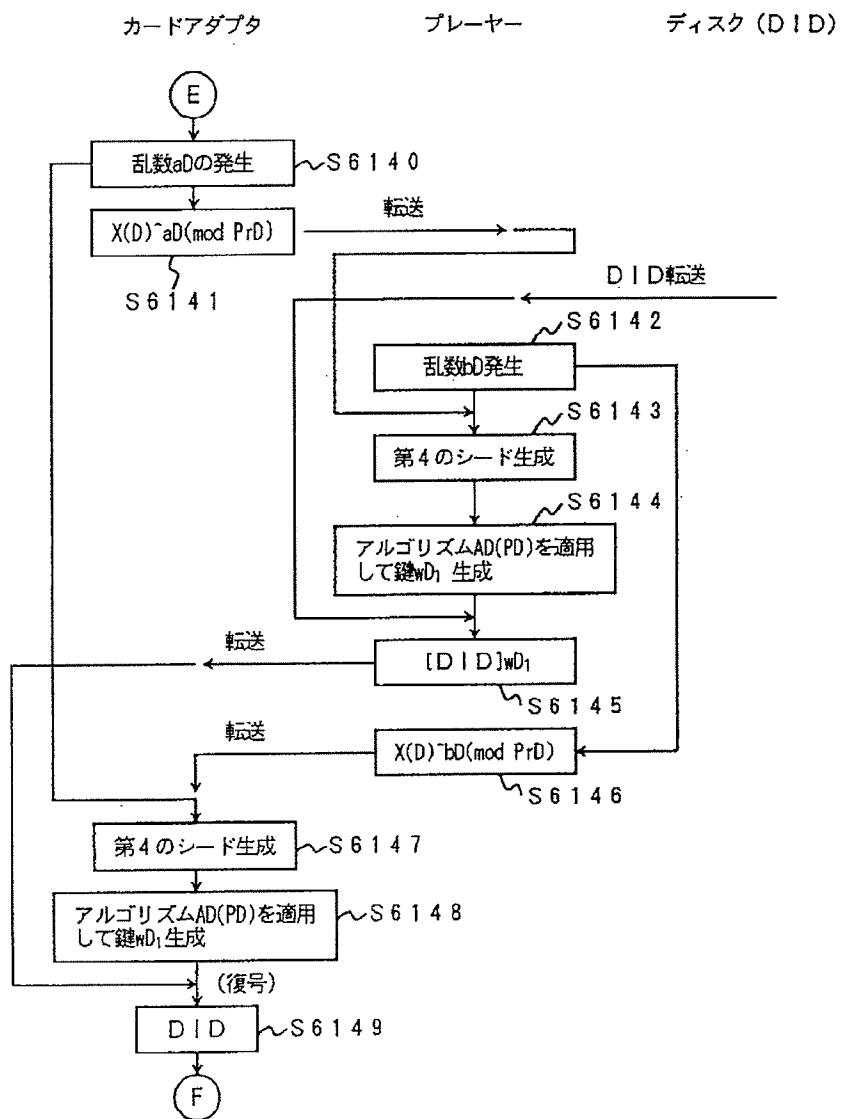
【図142】



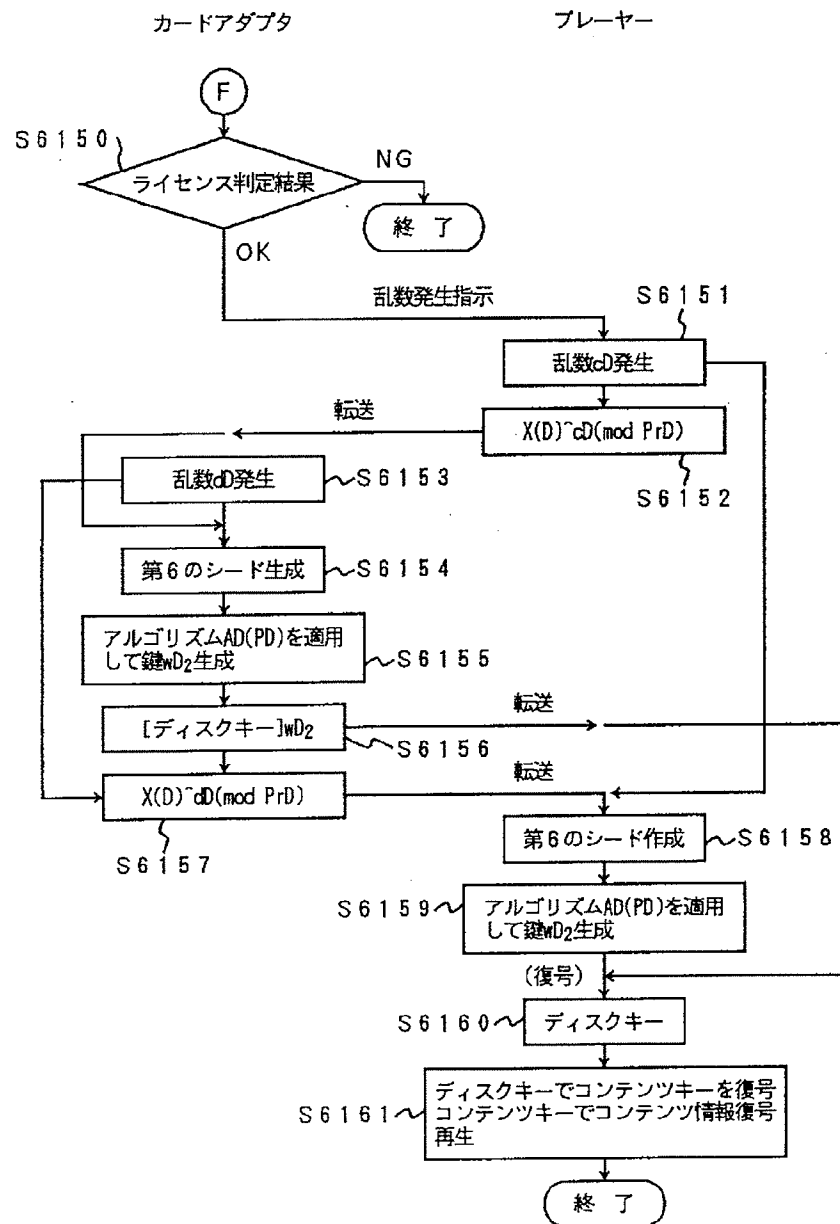
【図143】



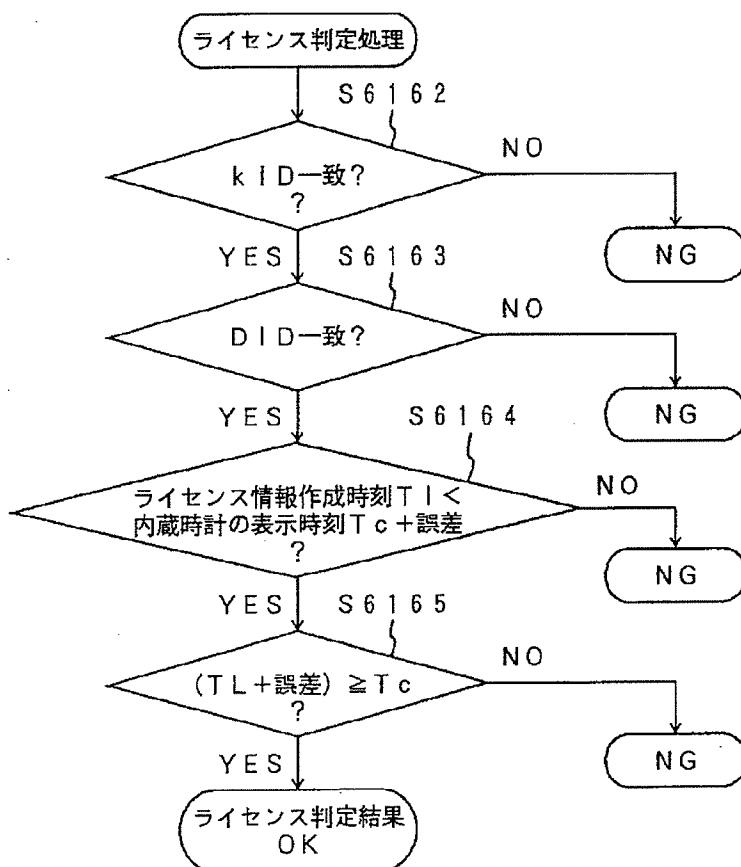
【図144】



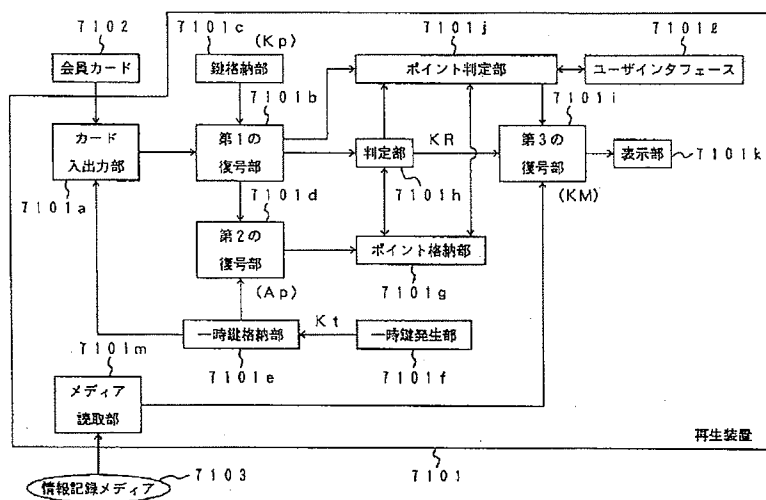
【図145】



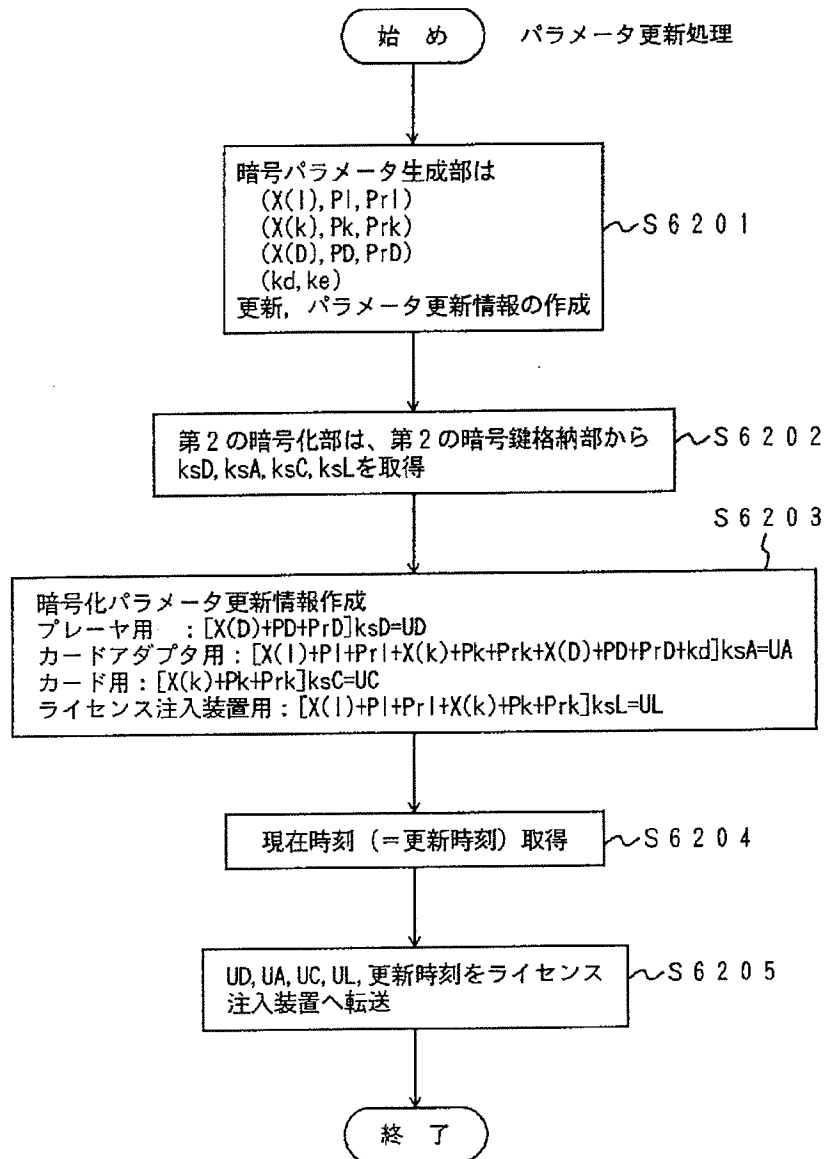
【図146】



【図152】

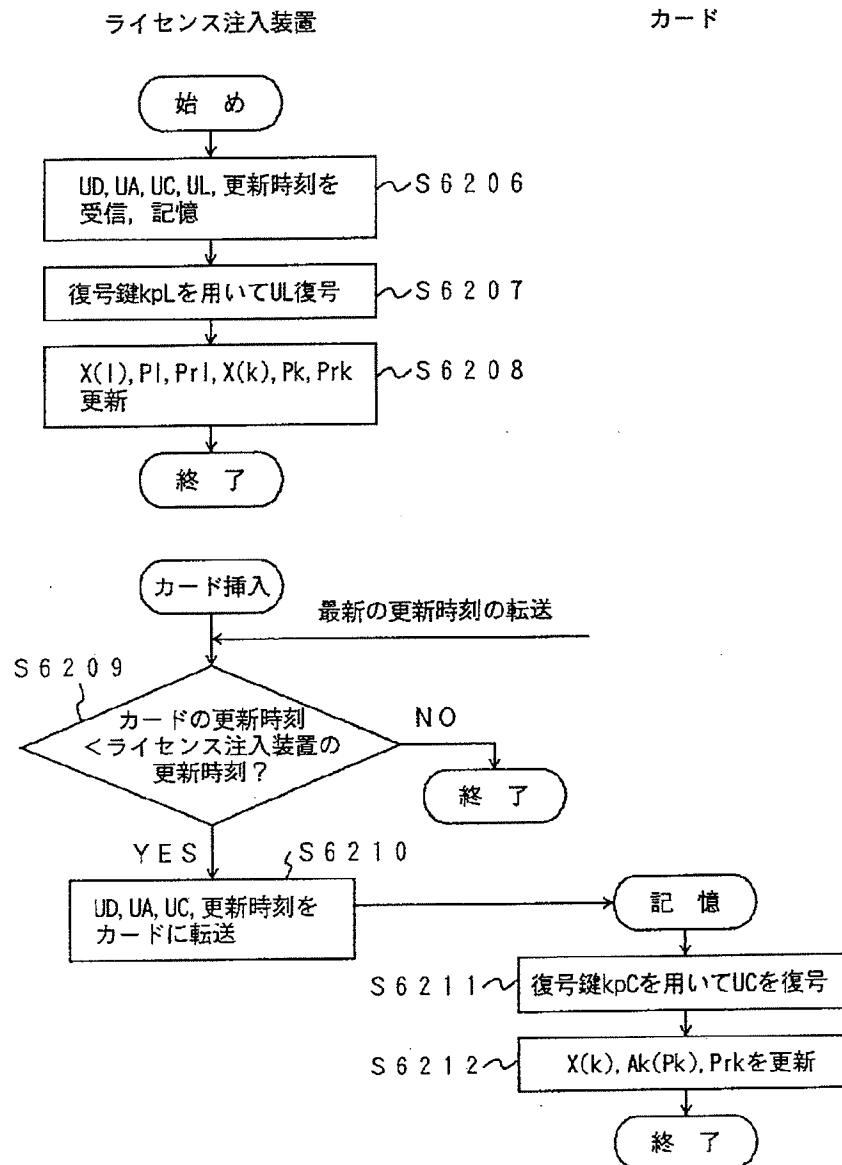


【図147】

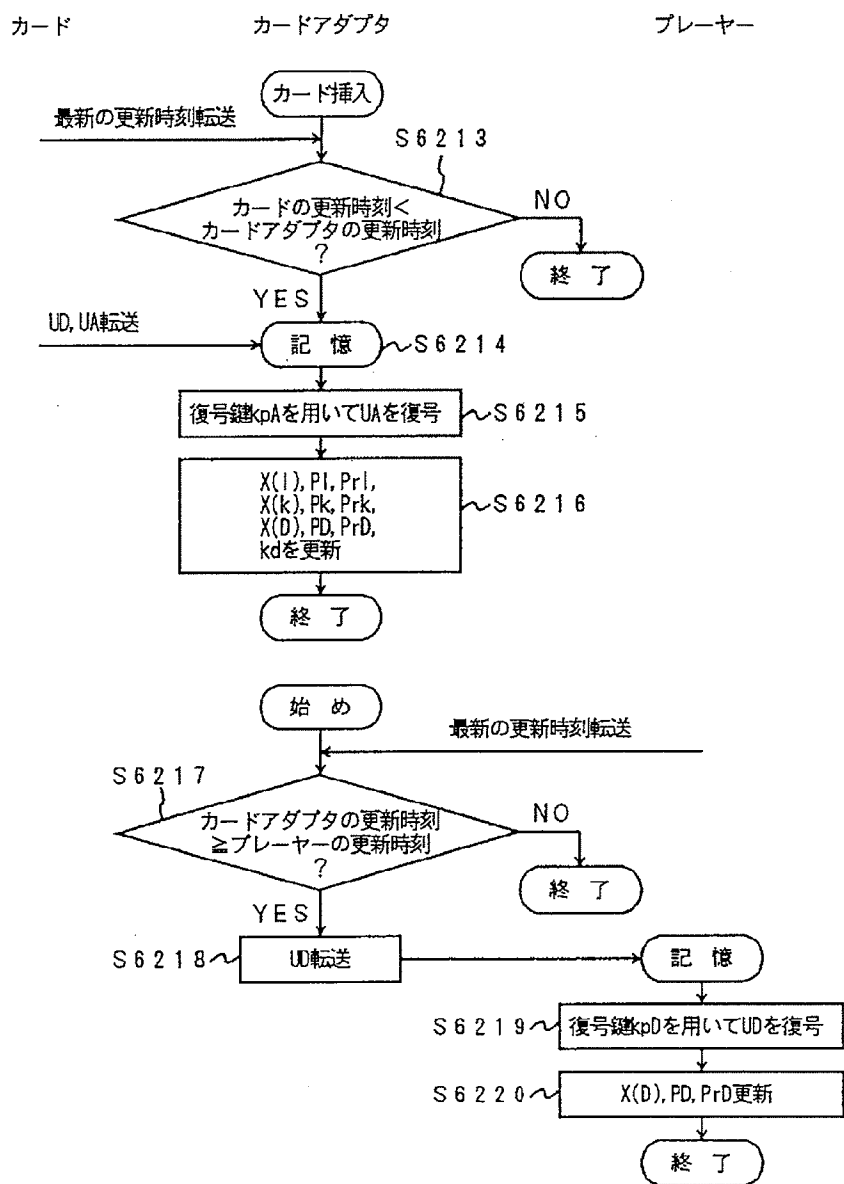




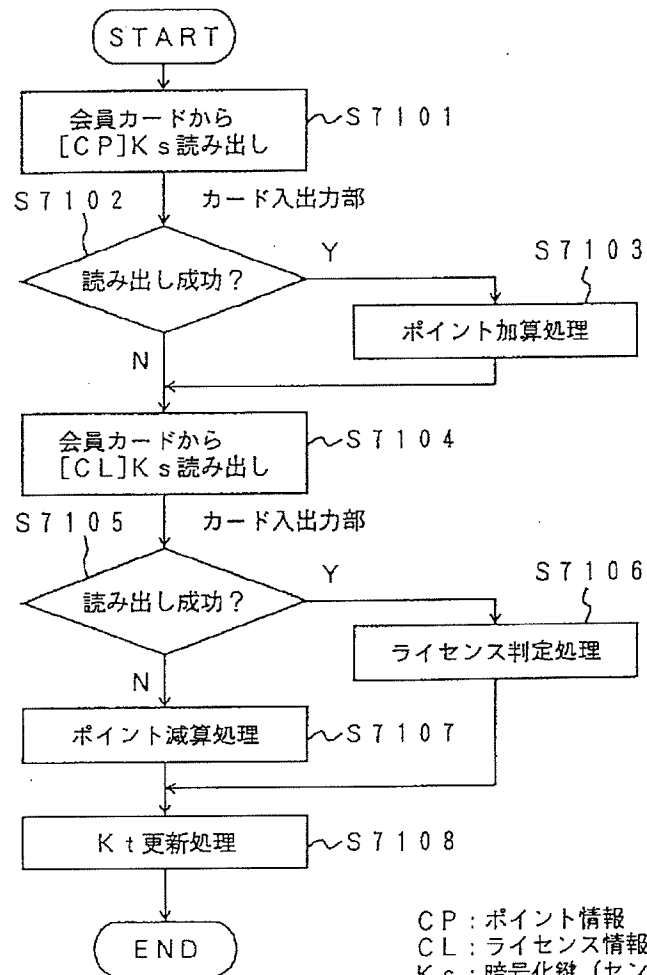
【図148】



【図149】

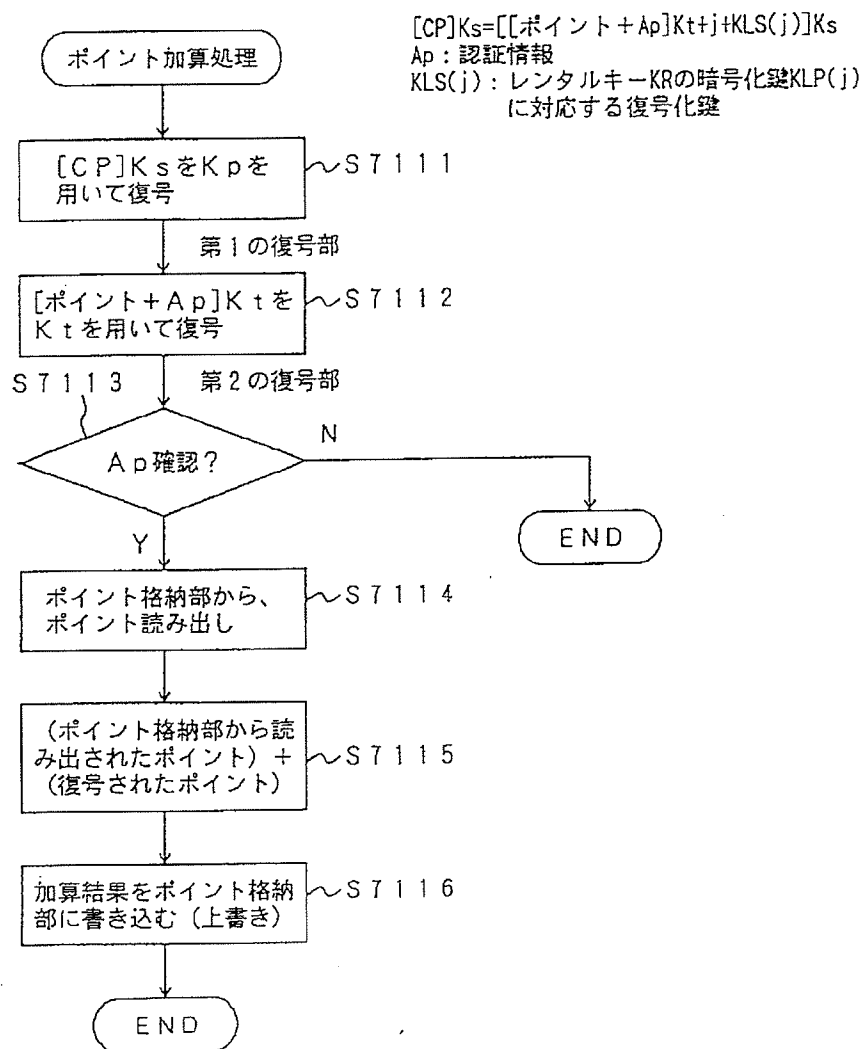


【図153】

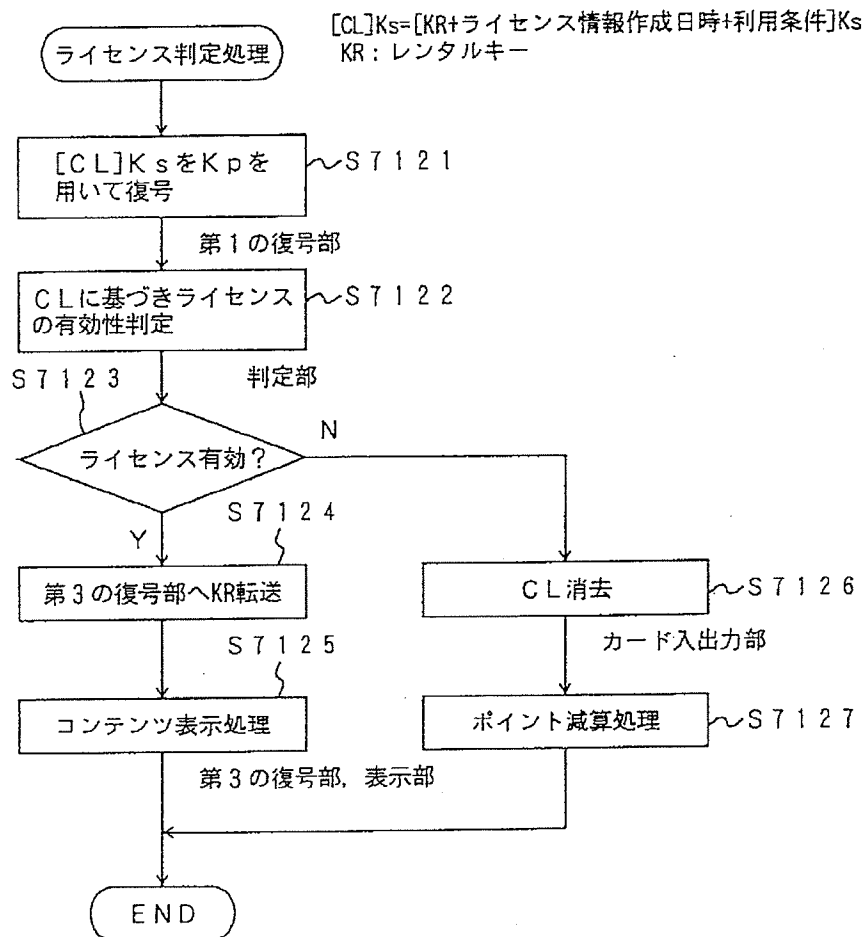


CP: ポイント情報  
CL: ライセンス情報  
Ks: 暗号化鍵 (センター装置が保存)  
Kt: 秘密鍵 (再生装置が発生)  
Kp: 暗号化鍵Ksに対応する復号化鍵  
(再生装置が保持)

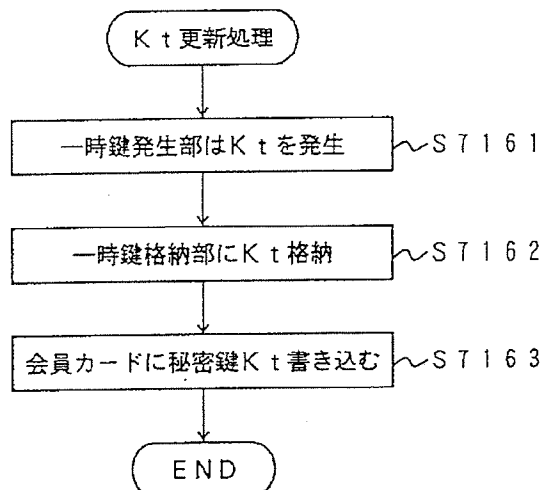
【図154】



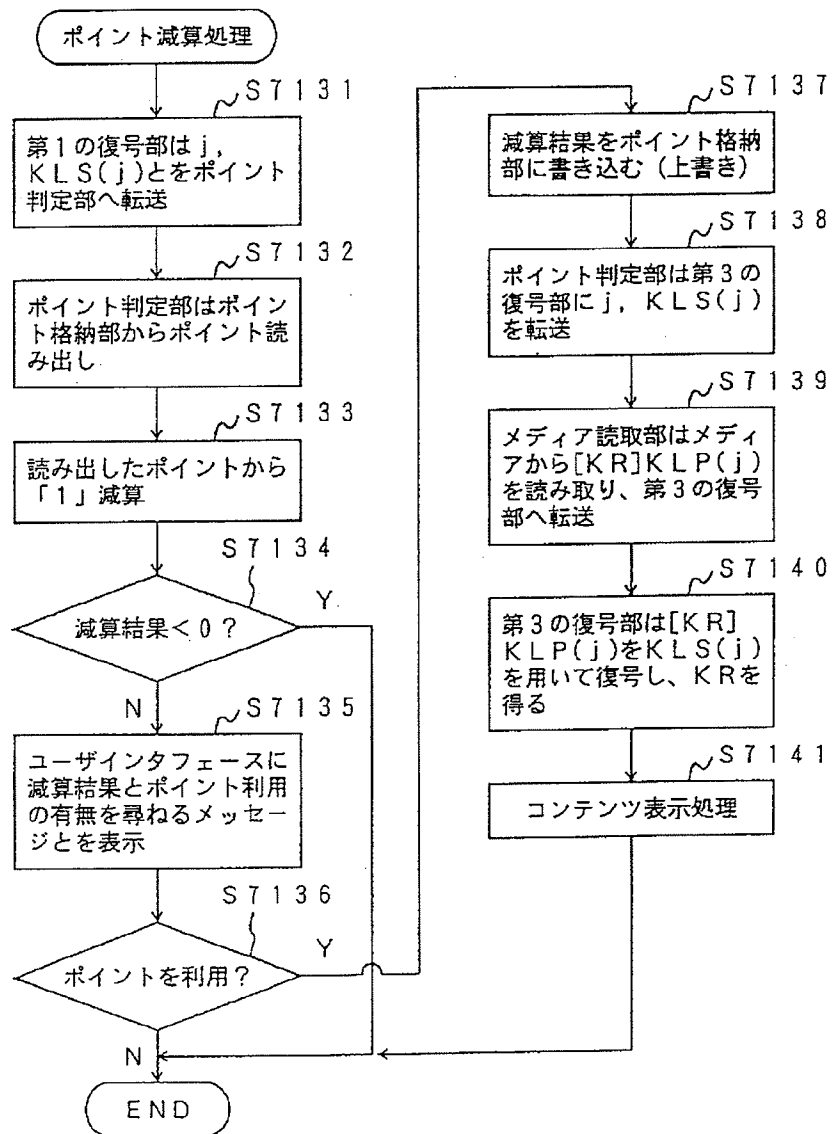
【図155】



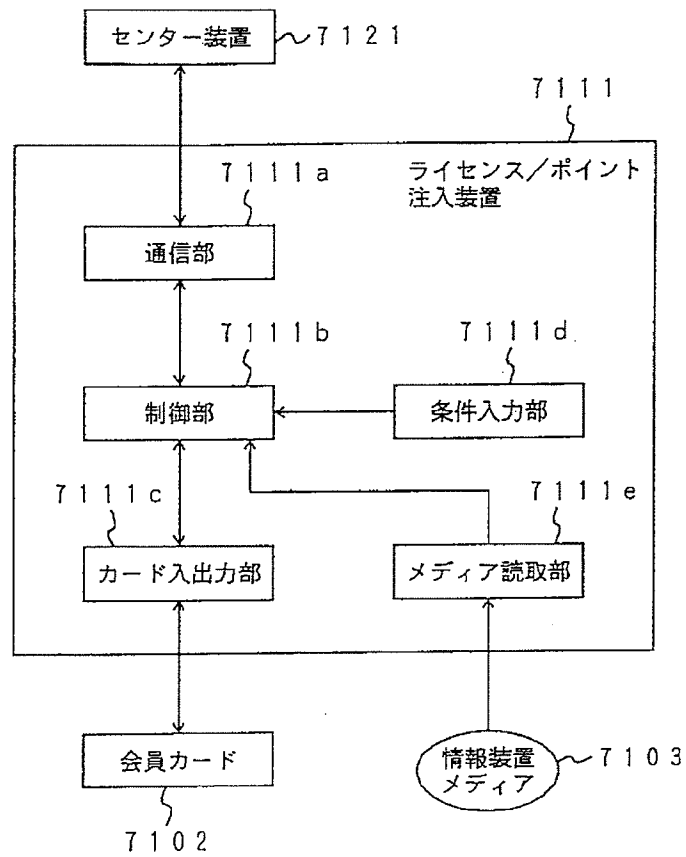
【図158】



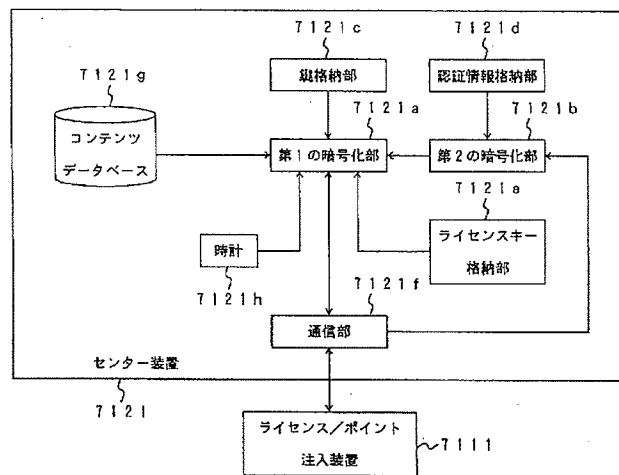
【図156】



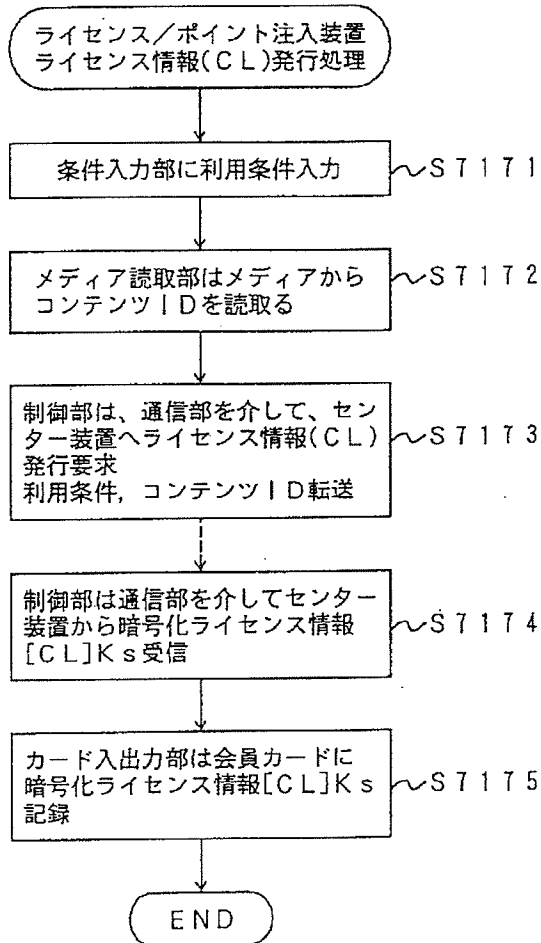
【図159】



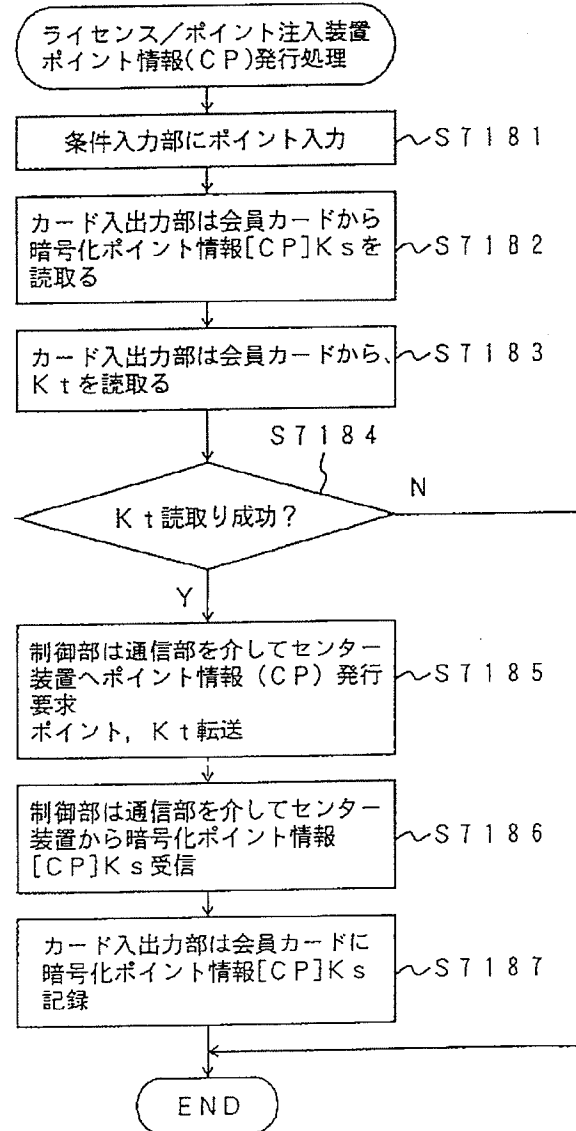
【図162】



【図160】

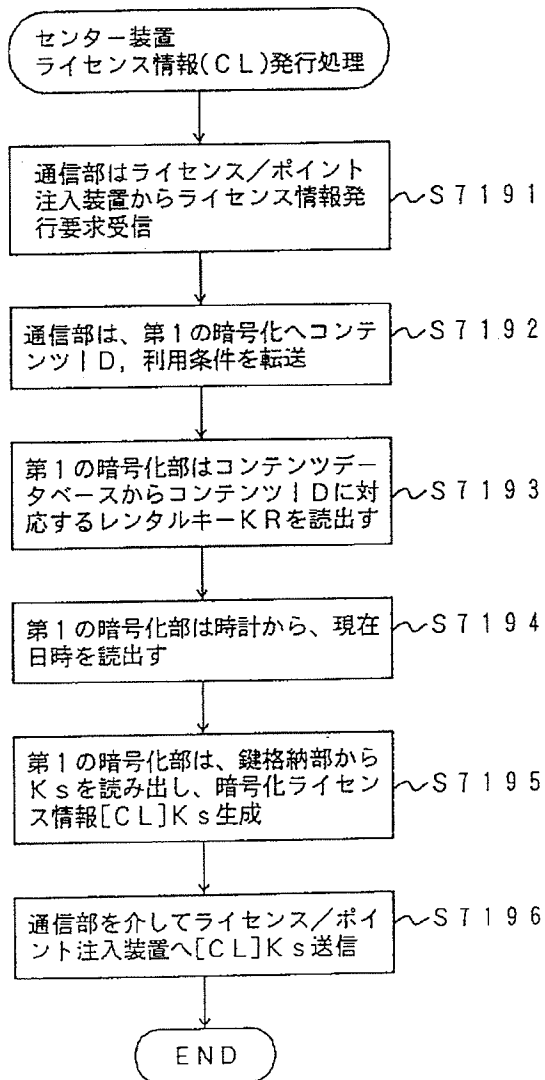


【図161】

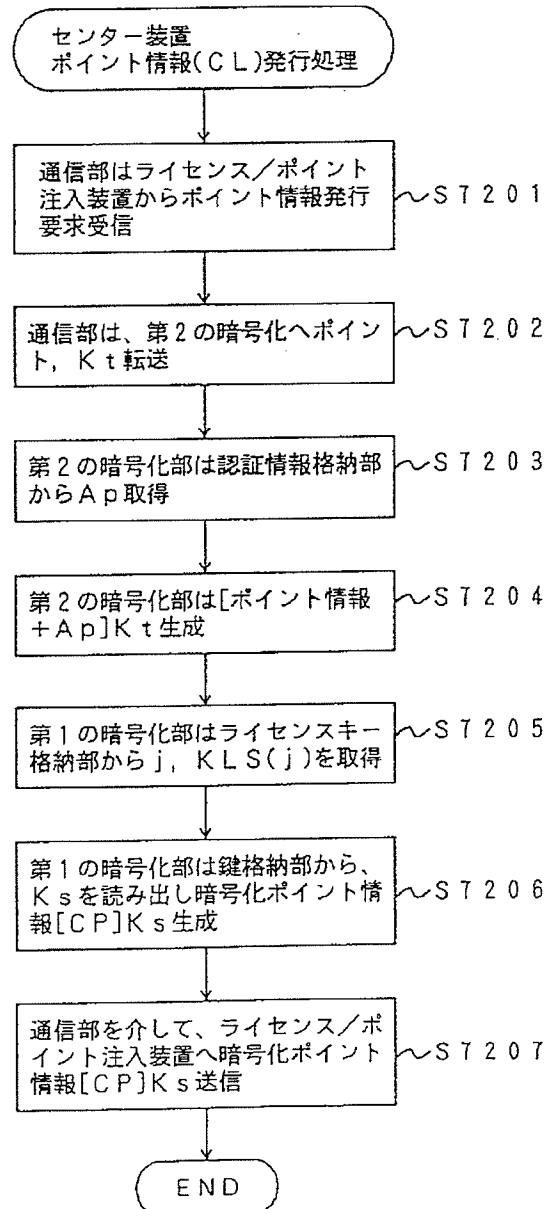




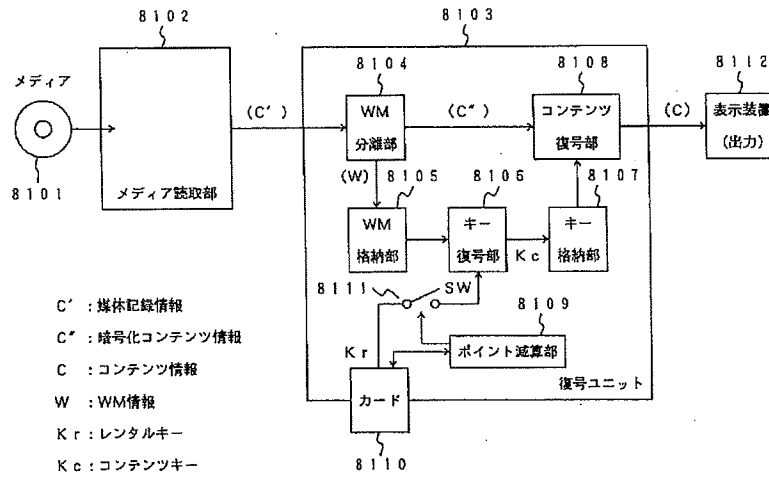
【図163】



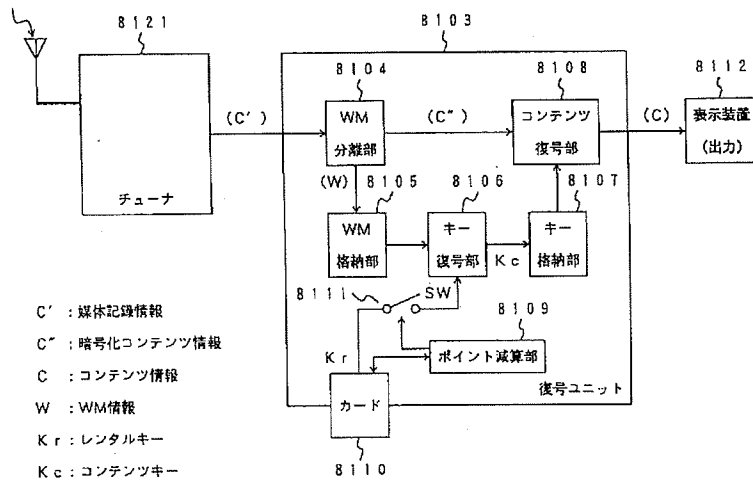
【図164】



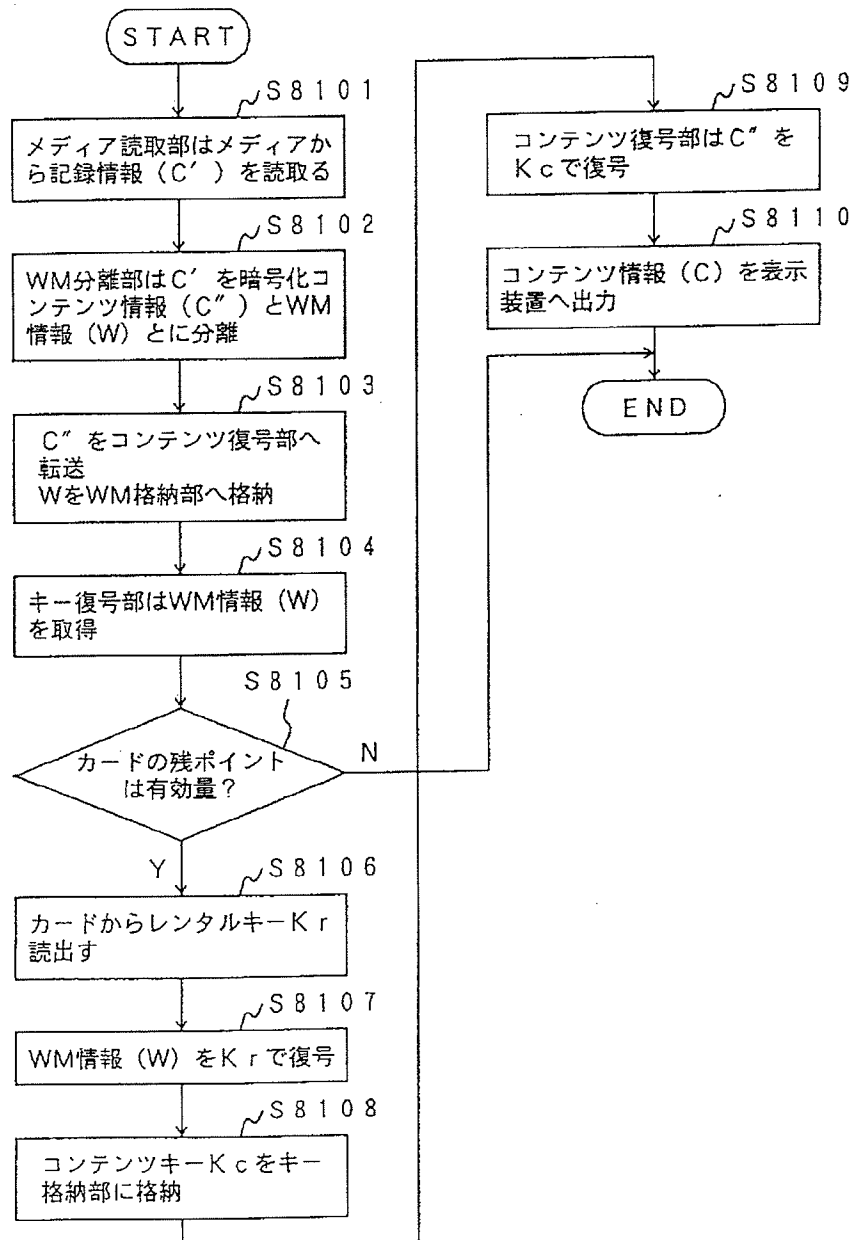
【図165】



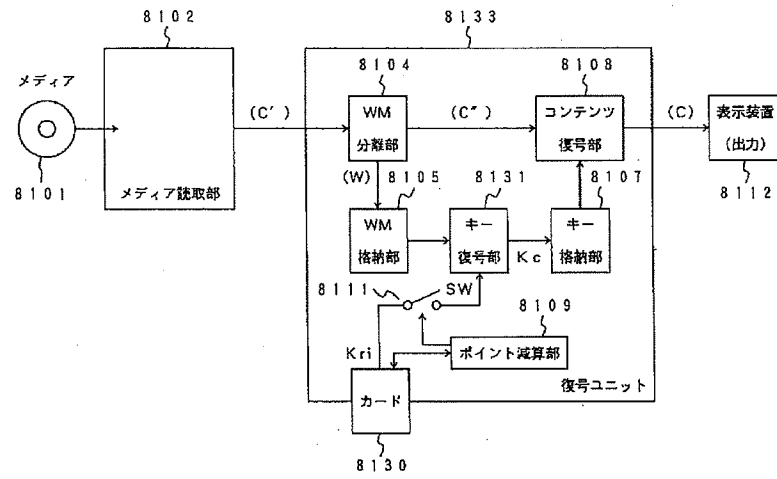
【図168】



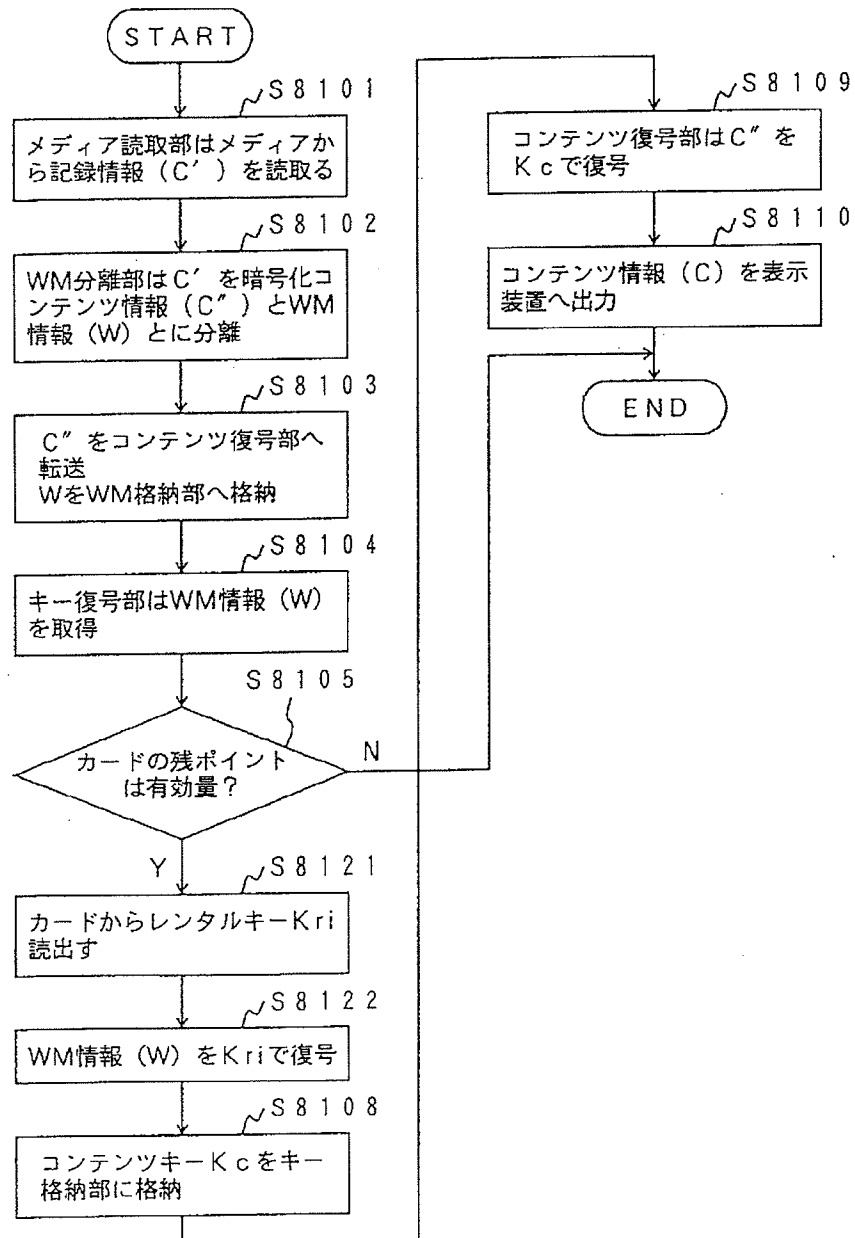
【図167】



【図169】



【図171】



フロントページの続き

(51)Int. Cl.<sup>6</sup>

G 0 6 F 13/00

// G 0 9 C 1/00

識別記号

3 5 1

6 6 0

F I

G 0 6 F 13/00

G 0 9 C 1/00

3 5 1 Z

6 6 0 D

(72)発明者 住田 一男  
神奈川県川崎市幸区小向東芝町 1 番地 株  
式会社東芝研究開発センター内

(72)発明者 平川 秀樹  
神奈川県川崎市幸区小向東芝町 1 番地 株  
式会社東芝研究開発センター内

(72)発明者 菅谷 寿鴻  
神奈川県川崎市幸区小向東芝町 1 番地 株  
式会社東芝研究開発センター内

(72)発明者 梶浦 正浩  
神奈川県川崎市幸区小向東芝町 1 番地 株  
式会社東芝研究開発センター内